INSTITUTO TECNOLÓGICO DE COSTA RICA

ESCUELA DE INGENIERIA ELECTRÓNICA

Superintendencia General de Entidades Financieras
SUGEF

"Diseño de un modelo lógico y su plan de migración para la reestructuración de la red de la SUGEF"

Informe de Proyecto de Graduación para optar por el Grado de Bachiller en Ingeniería en Electrónica

Alejandro Román Acuña

CARTAGO 2001

RESUMEN

La información que manejan las empresas hoy en día es muy sensitiva, para que cualquier tipo de persona pueda ingresar a ellas, incluso en la misma empresa. Por eso existen diferentes niveles de seguridad para usuarios de una misma red y niveles de seguridad mucho más estrictos para usuarios externos autorizados y no autorizados.

La red de área local de una empresa debe mantener estrictos niveles de seguridad, para que los diferentes usuarios dentro de la misma empresa no tengan acceso a servidores e información que allí se encuentra y que no compete al trabajo que ellos realizan.

Por eso, cuando se diseña una segmentación lógica de una red es necesario definir perfiles tanto de usuario como de servidores, para identificar exactamente cual ingreso realizan los usuarios a los servidores y que tipo de información accesan. Para resolver este problema los equipos de red actuales permiten realizar diseños de LAN virtuales (VLAN), que permiten crear una red dentro de un mismo equipo de red sin necesidad de gastar más recursos, pero incrementando la seguridad y eficiente uso de la red.

Pero al realizar este diseño se debe tener claro como está estructurada la red, se debe analizar aspectos de diseño físico del edificio, características técnicas del equipo, protocolos de enrutamiento, cableado estructurado, entre otros, para conocer realmente si ese cambio es necesario y en cuanto puede impactar ese cambio a la red para su funcionamiento correcto.

Luego del análisis de todas estas variables, es necesario realizar un plan de migración adecuado al tiempo y dedicación del personal encargado del área de datos, teniendo en cuenta que para el usuario este cambio debe ser transparente y asegurar el monitoreo y correcto funcionamiento una vez realizado el cambio.

Por último se investigaron las tecnologías existentes de VoIP y las características de calidad de servicio que debe cumplir esta para que pueda ser implementado sobre el diseño lógico propuesto y sobre el equipo actual que tiene la red.

Palabras claves: segmentación lógica, VoIP, VLAN, protocolo de enrutamiento

ABSTRACT

The information that handles the companies nowadays is very sensitive, so that any type of person can enter them, even in the same company. For that reason different levels from security for users of a same network and much more strict levels of security for external users exist authorized and non authorized.

The local area network of a company must maintain strict levels of security, so that the different users within the same company do not have access to servers and information that is there and that it is not incumbent on to the work that they make.

For that reason, when a logical segmentation of a network is designed is necessary to as much define profiles of user as of servers, to identify exactly as entrance they make the users to the servers and who type of information get in. In order to solve this problem the present equipment of network allows to make virtual designs of LAN (VLAN), that allows to create a network within a same equipment of network with no need to spend more resources, but increasing the security and efficient use of the network.

But when making this design is due to know clearly as the network is structured, is due to analyze aspects of physical design of the building, technical characteristics of the equipment, routing protocols, structured wiring, among others, to really know if that change is necessary and as soon as it can hit that change to the network for his correct operation.

Soon of the analysis of all these variables, it is necessary to make a plan of migration adapted to the time and dedication of the personnel in charge of the area of data, considering that stops the east user change must be transparent and to assure the monitoring and correct operation once made the change.

Finally the existing technologies of VoIP and the characteristics of quality were investigated on watch that must fulfill this so that it can be implemented on the proposed logical design and the present equipment that the network has.

Keywords: VoIP, VLAN, rounting protocols, logic design

DEDICATORIA

Agradezco a Dios y a mis padres por todo su apoyo, confianza y guía que me han brindado a través de toda mi vida.....muchas gracias.....

AGRADECIMIENTO

Agradezco a mi gran amigo el Ing. Kennett Espinoza por toda su ayuda desinteresada que siempre me ha brindado, no importa el momento ni el lugar, y que la frase “el que encuentra un amigo encuentra un tesoro” es una absoluta verdad.

También quiero agradecer a Carlos Chian y Marlon Morales por esos grandes años de amistad que hemos tenido a través del estudio y ahora en nuestra nueva etapa como profesionales.

Por último agradecer al Ing. Jaime González y Víctor Corrales por su ayuda en la práctica profesional y es especial al Ing. Juan Carlos Soto por haberme brindado un ejemplo a seguir como profesional y como persona, y por todos esos consejos tan valiosos que los voy a tomar muy en cuenta.

INDICE GENERAL

INDICE DE FIGURAS

INDICE DE TABLAS

CAPITULO 1
INTRODUCCION

1.1 Descripción de la empresa

La Superintendencia General de Entidades Financieras (SUGEF) es un órgano de desconcentración máxima del Banco Central de Costa Rica, creado por la Ley 7558, Ley Orgánica del Banco Central de Costa Rica, y modificado por la Ley 7732, Ley Reguladora del Mercado de Valores. Su misión es velar por la estabilidad, la solidez y el funcionamiento del Sistema Financiero Nacional, con estricto apego a las disposiciones legales y reglamentarias aplicables.

Están sujetos a su fiscalización los bancos comerciales públicos y privados, las empresas financieras no bancarias, las organizaciones cooperativas de ahorro y crédito, las mutuales de ahorro y préstamo y las casas de cambio, así como las entidades autorizadas por ley para realizar intermediación financiera o participar en el mercado cambiario.

La SUGEF está conformada por cinco Direcciones Generales subdivididas en departamentos como se muestra en la Tabla 1.1.

La Superintendencia General de Entidades Financieras funciona bajo la dirección de un órgano denominado Consejo Nacional de Supervisión del Sistema Financiero, integrado por el Ministro de Hacienda o, en su ausencia, un Viceministro de esa cartera, el Presidente o el Gerente del Banco Central de Costa Rica y cinco miembros, que no serán funcionarios públicos, nombrados por la Junta Directiva de esa entidad bancaria por un periodo de cinco años y que podrán ser reelegidos por una sola vez. Entre ellos y por periodos de dos años, el Consejo Nacional elegirá a su Presidente, el cual también puede ser reelecto.

Tabla 1.1 Distribución departamental de la SUGEF

DIRECCIÓN GENERAL	DEPARTAMENTOS
Inspección de Bancos (1)	► Inspección de Bancos Privados y Grupos Financieros ► Inspección de Públicos
Instituciones Financieras No Bancarias (1)	► Inspección de Instituciones Financieras no Bancarias ► Inspección de Cooperativas
Análisis Financiero	► Análisis Financiero de Bancos ► Intermediarios Financieros no Bancarios ► Servicios Técnicos
Administrativa	► Servicios Administrativos ► Recursos Humanos
Asesoría Jurídica	

(1) A cargo de las inspecciones "in situ" de las entidades sujetas a supervisión.

El superior jerárquico de la Superintendencia es el Superintendente General quien, en su ausencia, es sustituido por el Intendente General. Ambos funcionarios, nombrados por el Consejo Nacional por períodos de cinco años, pueden ser reelectos.

Las principales responsabilidades de las Direcciones Generales son las siguientes: dirigir las actividades y tareas asignadas a su esfera de acción, transmitir al personal a su cargo las directrices y las políticas generales que emanan del máximo jerarca de la Institución, servir de filtro técnico especializado para que los trabajos que debe aprobar y suscribir el Superintendente General reúnan las condiciones de calidad, cobertura y presentación adecuados, y asesorar al Superintendente en materias de su especialidad.

Además, conforman esta institución un Departamento de Informática y un Departamento de Auditoría Interna, la cual depende del Consejo Nacional de Supervisión y ofrece servicios de asesoría a la administración, para que ésta alcance sus objetivos con mayor eficiencia, proporcionando recomendaciones sobre las operaciones que examina en forma posterior.

El Departamento de Informática, en el cual es donde se está realizando el proyecto, está a cargo de las secciones “Soporte Técnico” y “Desarrollo y Mantenimiento de Sistemas”. Su objetivo es crear y mantener la infraestructura computacional necesaria para apoyar las labores de supervisión. Esto lo logra por medio de sus funciones básicas que son:

- Planeación y presupuestación de las necesidades de bienes y servicios informáticos.
- Desarrollo y mantenimiento de sistemas.
- Soporte técnico.
- Administración y control del proceso de recepción y carga de los datos que envían las entidades supervisadas.

En este departamento laboran 16 personas de las cuales hay 14 informáticos y dos ingenieros en electrónica. El jefe de departamento es el Msc. Fernando Aguilar y la persona que va a estar supervisando en el proyecto es el Ing. Jaime González y el Ing. Juan Carlos Soto, ambos ingenieros en electrónica en el departamento.

1.2 Definición del Problema y su importancia

La red datos de la SUGEF se empezó a gestar en el año de 1998 como un proyecto de renovación, cuyo fin era aumentar el rendimiento de los trámites de supervisión bancaria que allí se realizan y brindar a los empleados herramientas más eficaces de trabajo para la supervisión de entidades.

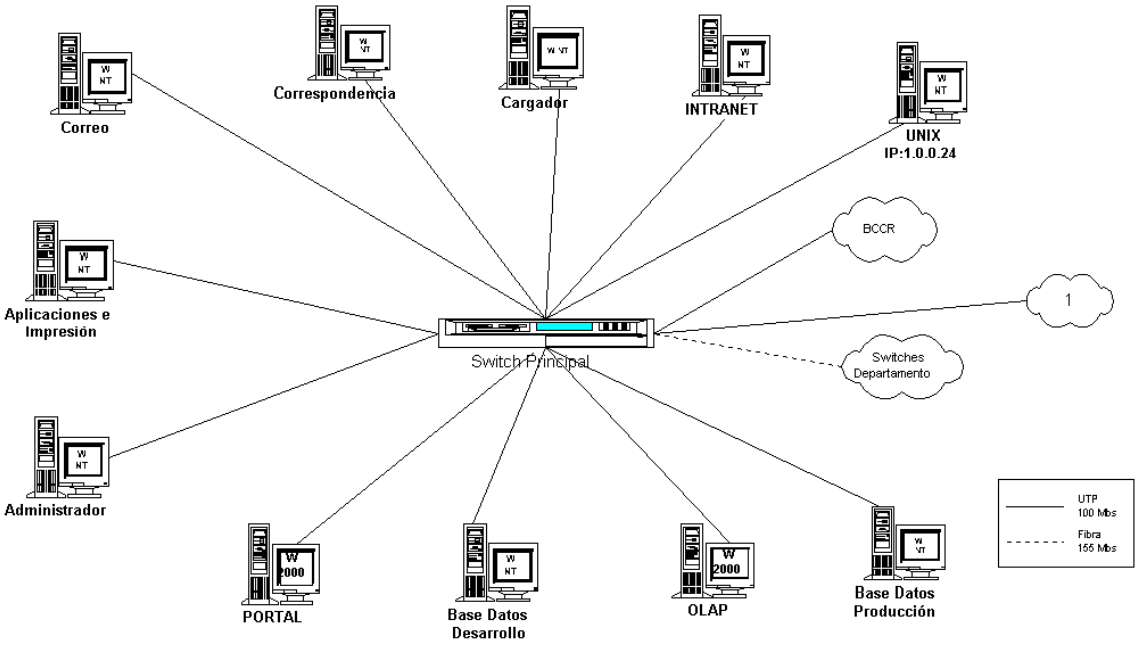


Figura 1.1 Distribución Actual de la Red de la SUGEF

La figura 1.1 muestra la parte principal de la red de la SUGEF. Al switch principal se encuentran conectados varios servidores que cumplen funciones específicas (OLAP por ejemplo) y algunos generales (aplicaciones e impresión, intranet entre otros). La conexión física entre el switch principal y los servidores es por medio de cable UTP a 100 Mbs..

Existe también una conexión a 100 Mbs con el Banco Central de Costa Rica de alta velocidad.

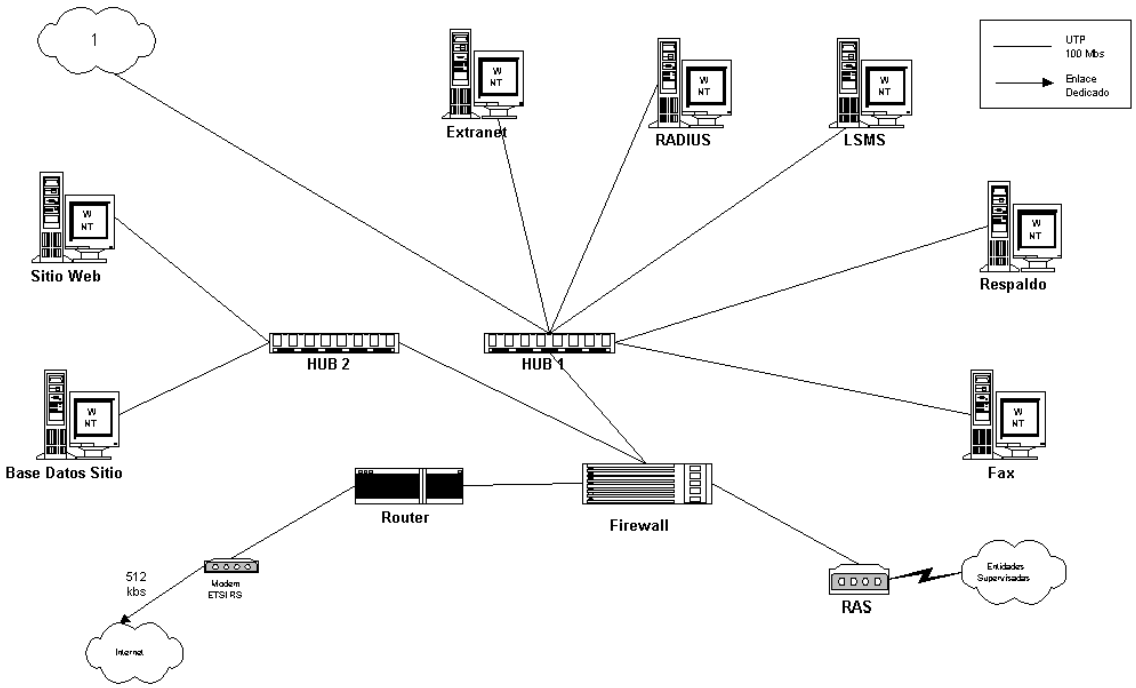


Figura 1.2 Continuación 1: Distribución Actual de la Red de la SUGEF

La figura 1.2 muestra la continuación de la distribución de la red. Un cable UTP a 100 Mbs que en la figura 1.1 y la figura 1.2 se encuentra dentro de una nube y numerado con un 1 (uno), es la conexión directa a otra parte importante de la red (figura 1.3)

Esta figura muestra a los servidores en los cuales las entidades financieras externas cargan sus archivos (extranet) por medio del RAS. También se encuentra los servidores de acceso por internet, los equipos que se requieren para conectarse a este servicio (router, modem) y su respectivo firewall como protección de la red externa a la interna.

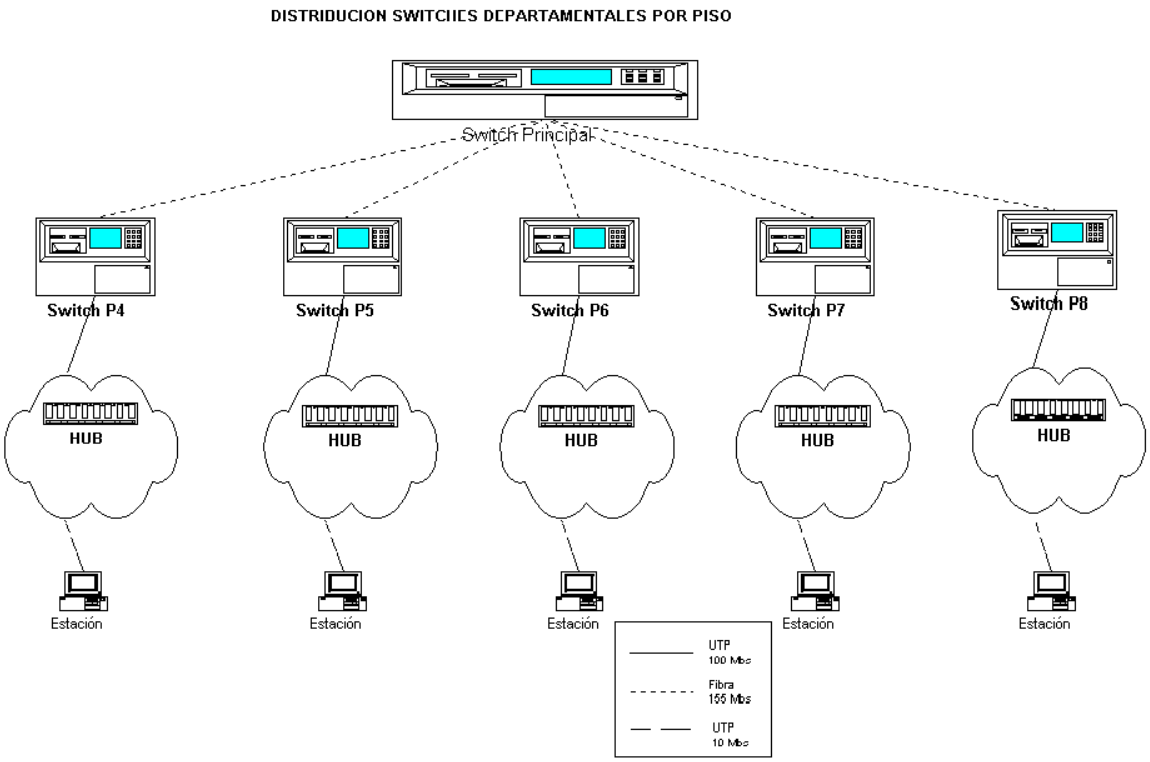


Figura 1.3 Continuación 2: Distribución Actual de la Red de la SUGEF

En el apéndice 1 se muestra la distribución física del edificio de la SUGEF y complementado con la figura 1.3 muestra que existe un switch departamental, en cada piso del edificio. Existe también una conexión física entre el switch departamental y principal de fibra óptica multimodo a una velocidad de 155 Mbs. Cabe destacar que solo existe un par de fibra óptica conectad, porque entre cada piso existe un par más.

Cada piso además del switch, cuenta con hubs de 12 puertos que hacen la distribución final a las estaciones de trabajo de cada empleado.

La red de la SUGEF maneja un grupo de direcciones clase B que fue otorgada por el Banco Central de Costa Rica y son las siguientes:

- 152.32.33..XX / 24
- 152.32.34..XX / 24
- 152.32.35.XX / 24
- 152.32.36.XX / 24

- 152.32.37.XX / 24

De este grupo solo se están utilizando las direcciones 152.32.33..XX /24, 152.32.34..XX / 24 y 152.32.35.XX / 24, las otras no se utilizan ni están configuradas en el switch principal. Actualmente no se puede distinguir cuales grupos de direcciones están asignados a servidores, y cual grupo está asignado a impresoras o usuarios. Aquí se presenta el primer problema del proyecto, ya que conforme fue creciendo la entidad, se han ido asignando direcciones IP a usuarios, servidores e impresoras sin ningún orden. Por ejemplo, se pudo determinar que hay usuarios con direcciones 152.32.33..5, luego el servidor Faxination con dirección IP 152.32.33..8 y una impresora del piso 6 con dirección IP 152.32.33..20.

Esto creó en la SUGEF una incertidumbre en el manejo de la red, porque no existe un control ni documentación indicando como está organizada la red, los cambios y cuales son los pronósticos de crecimiento de usuarios, servidores e impresoras.

El problema que se presentó, es consecuencia de otro problema que va relacionado directamente con el switch principal y los de distribución departamental. El protocolo de enrutamiento que maneja la red es RIP (routing internal protocol) versión 1, donde este protocolo entre otras características no permite el "subnetting", es decir, de nada hubiera servido realizar grupos para organizar la red, si el protocolo de enrutamiento no lo permite. Se puede observar otras características del protocolo RIP versión 1 en el apéndice 3.

El modelo lógico de la red o diseño de las VLAN de cada switch, confirma el problema de no realizar ningún subneteo, debido a que solo existen tres VLAN, una para cada dirección que se está utilizando y se repite lo mismo para cada switch departamental. Toda la información viaja por un mismo tubo sin distinción, creando un problema grave ante circunstancias especiales, técnicamente se llama broadcast domain. (dominio de colisión), que puede llegar hasta colapsar a la red.

La prioridad de reestructurar la red desde el punto de vista lógico, es una necesidad latente, ante el tipo y cantidad de información que la empresa maneja. Además, se va iniciar a brindar servicios por Internet a diferentes entidades financieras del país, lo que agudiza el problema. Es necesario realizar un diseño que permita administrar todos los componentes de hardware y software existentes dentro de la red, con la finalidad de afrontar la complejidad y el crecimiento paulatino que se ha generado, de modo que se pueda optimizar la capacidad de los recursos disponibles para un mejor aprovechamiento de los mismos.

1.3 Objetivos

1.3.1 Objetivo General

Generar la segmentación lógica de distribución de la red y los procedimientos de implementación para la migración hacia este nuevo modelo. En un lapso de 16 semanas.

1.3.2 Objetivos Específicos

a. Investigar y conocer que son y como se manejan el protocolo de enrutamiento RIP.
b. Investigar y conocer que son y como se manejan el protocolo de enrutamiento OSPF
c. Aprender las aplicaciones y características de los switches Xylan.
d. Investigar y documentar la estructura actual de la LAN de la SUGEF
e. Crear perfiles de usuario y servidores según la actividad que realizan.
f. Diseño del modelo lógico de la red
g. Escogencia del nuevo protocolo de enrutamiento
h. Realización programación básica del protocolo de enrutamiento escogido en el switch Xylan en modo laboratorio.
i. Estudio del impacto de la red ante el cambio del protocolo de enrutamiento.
j. Realizar un plan de migración de la reestructuración de la red.
k. Realizar un diseño del modelo lógico y físico para lograr integrar la tecnología de VoIP en la red de la SUGEF.

CAPITULO 2
ANTECEDENTES

2.1 Estudio del problema a resolver

Los aspectos a un nivel macro se pueden clasificar en tres grandes grupos:

1- Análisis de la red actual

2- Propuesta de red nueva

3- Diseño de una red básica para implementar VoIP.

Con relación al primer punto, se investigó las características de la red que actualmente la entidad no tenía. No existía un diagrama físico de la red y no se conocía con certeza la distribución de direcciones. Se analizó otros aspectos como el tipo de personal que trabaja en la SUGEF, y con ello determinar perfiles de usuario, para luego poder crear una segmentación lógica.

También, se realizó la distribución de dispositivos conectados al backbone de la entidad y diagramas de localización de los departamentos por pisos y del equipo que se encuentra en cada piso.

La propuesta nació del análisis de la red actual. Se consideró en primera instancia, el papel que juega cada servidor en la misma, ligado a las tareas que realiza cada usuario que existe en la red. Se tomó como criterio de diseño, que no todos los usuarios deben ingresar o tener acceso a todos servidores. Hay cierta cantidad de usuarios que solo ingresan a un servidor y no existe razón para que puedan accesar a otros servidores. Con el análisis que se realizó, se concluyó la propuesta y una nueva segmentación lógica de la red. También esta segmentación lógica, implicó la necesidad de un cambio de software en los sistemas operativos de los switches de la SUGEF.

Por último, el tercer punto, fue considerar los aspectos básicos de una implementación de la tecnología de VoIP en la red propuesta. Aquí otra vez se requirió hacer análisis de perfil de usuario, además de una investigación de cual era el equipo que existe en el mercado, y cual se necesitaba para lograr implementar la tecnología de VoIP en la red de la SUGEF.

2.2 Requerimientos de la empresa

La SUGEF a partir de este proyecto de graduación espera obtener la segmentación lógica de distribución de la red, además de procedimientos para la implementación de la migración hacia una red más óptima y segura. Para lograrlo se han propuesto una serie de requisitos que se deben satisfacer, tales como:

a. Una adecuada administración de los siguientes dispositivos:
    - Servidores
    - Estaciones de Trabajo
    - Switches Xylan (Omniswitch y Omnistack).
    - Hubs
    - Enlaces Internet
    - Accesos Remoto
b. Control de Ingresos de funcionarios y entidades bancarias por Internet.
c. Plan de migración controlado
d. Uso de plataformas de monitoreo de dispositivos de la red (X-Vision)
e. Distribución de perfiles por usuario.

2.3 Solución Propuesta

La primera propuesta se refirió a la investigación de los diferentes protocolos de enrutamiento que existen en el área de redes. Se investigaron los protocolos RIP versión 1, RIP versión 2 y OSPF. El primer protocolo se investigó debido a que este protocolo es el instalado en los switches y no se conocía técnicamente su funcionamiento. Los otros dos protocolos RIP versión 2 y OSPF son protocolos nuevos y mejores que el RIP versión 1 y para lograr una reestructuración de la red más óptima (mayor información ver apéndice 3, apéndice 4 y apéndice 5), es necesario el cambio del protocolo de enrutamiento y su justificación se encuentra en la sección de análisis de resultados.

Luego de la investigación de protocolos, se procedió a realizar una serie de investigaciones de la estructura física del edificio, cantidad de usuarios, aplicaciones utilizadas, estructura física y segmentación lógica de la red.

Con la información obtenida de las investigaciones anteriores, se presentó los primeros diseños de los grupos y VLANs, denominado como el diseño de la segmentación lógica. Se dividieron a los usuarios por perfiles y a los servidores de acuerdo a su función en la red. También se tomó otros aspectos como impresoras, entidades bancarias externas y el grupo de auditoría que requiere accesos especiales y cuyo criterio de diseño, fue que que ellos lograran ver la red de la SUGEF, pero que cualquier usuario de la red de la SUGEF, no logre ingresar a la red de auditoría.

Cuando se logró segmentar a toda la red, se realizó la distribución del direccionamiento IP. Este se identificó de acuerdo al perfil y la cantidad de usuarios que este contenía, al igual se realizó con los servidores y grupos especiales, tomando en cuenta las direcciones que maneja la red.

Con la segmentación ya realizada y con la investigación de equipos hecha, se procedió a realizar el manual de migración de la red vieja a una nueva red. Se tomó en cuenta aspectos desde redireccionamiento IP de servidores, impresoras,

por ejemplo, hasta el cambio de asignar direcciones de una manera estática a dinámica, seguidas por políticas definidas (D.H.C.P.)

Uno de los últimos aspectos del proyecto, fue la integración de la tecnología de VoIP en la red. Se analizó aspectos de ancho de banda, calidad de servicio y el equipo actual, concluyendo en una serie de recomendaciones y características que debe presentar la red para poder soportar la tecnología antes mencionada, además de ciertas modificaciones que se deben realizar para tratar de sacar el mayor provecho a la red actual.

CAPITULO 3
PROCEDIMIENTO METODOLOGICO

La metodología seguida para el cumplimiento de los objetivos se presenta por medio de un diagrama de flujo para facilitar su realización y su comprensión, en la figura 3.1.

Como un breve repaso del diagrama de flujo, por la ineficiencia de un protocolo de enrutamiento (RIP 1), la red de la SUGEF no creció ordenadamente y debido a esto se empezó realizar un desorden en la asignación de direcciones. Como resultado de todo esto, nunca se llegó a realizar diagramas físicos ni lógicos de la red, por lo que se puede decir que la reestructuración de la red es casi como empezar de nuevo el diseño de la red.

Se tomaron variables, como son, los métodos de conectividad a los servidores y clientes (por ejemplo). Aunque estos ya estaban determinados por la red actual, se necesitaron evaluar para determinar que tan útiles son y además, realizar conclusiones efectivas para la solución del problema y si no, realizar recomendaciones para un futuro cercano.

También se realizó un plan de migración que toma en cuenta el cambio de direcciones estáticas a dinámicas (DHCP), y el redireccionamiento IP de toda la red actual, que incluyó servidores, usuarios, switches e impresoras.

Con este punto terminado se procedió a determinar si la red es capaz de soportar toda la tecnología de VoIP, tomando en cuenta el equipo utilizado actualmente en la red y el equipo que sería necesario agregar para lograr que esta tecnología funcione con los estándares básicos que esta necesita.

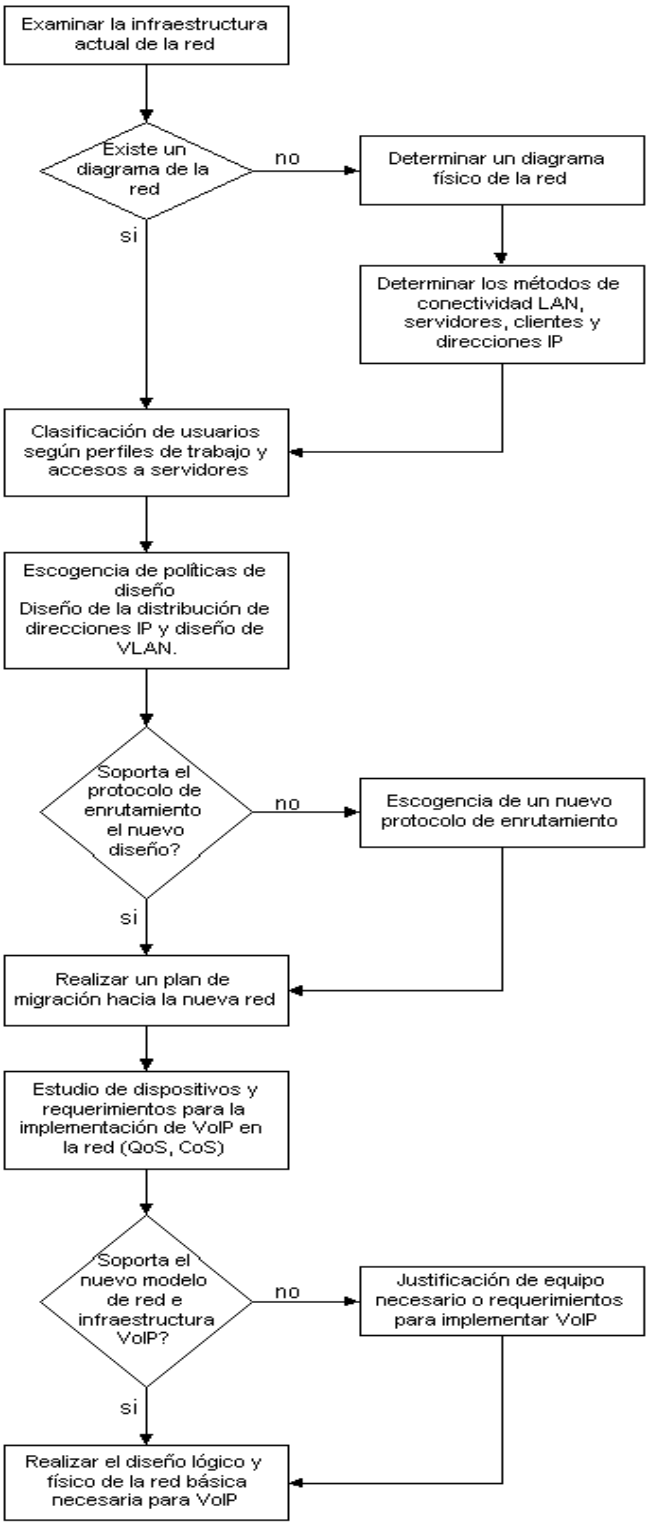


Figura 3.1 Proceso para determinar la estrategia de conexión a redes.

CAPITULO 4
DESCRIPCION DEL HARDWARE UTILIZADO

Principalmente el hardware utilizado se refiere a la utilización de los switches de capa 3 marca Xylan, modelo Omnistack 5024. Con este switch, se cumplió con el objetivo de realizar la programación para la migración del protocolo de enrutamiento de la versión 1 de RIP a la versión mejorada RIP v2 en modo laboratorio. Mayor información técnica de descripción y características se encuentran las hojas de datos en el anexo 2.

Para realizar la programación, se necesitó de una PC conectada por medio de un cable RS-232 en el puerto de consola del switch y en la PC en el COM 1 o COM2. Por este medio se pudo cargar o modificar el programa GATE-D el cual es el que permite establecer las características básicas del protocolo de enrutamiento a utilizar.

Para realizar las modificaciones de creación, modificación y actualización de VLAN, se puede realizar por medio de una PC y el programa TELNET. Aquí solamente se ingresa la dirección del switch y digitando un password se accesa a un menú con diferentes opciones que por medio del manual de usuario, se realiza las modificaciones necesarias según la propuesta de red.

CAPITULO 5
DESCRIPCION DEL SOFTWARE UTILIZADO

5.1 Introducción

El GateD es el software utilizado por los switches Xylan para establecer diferentes características de configuración como filtros, protocolos de enrutamiento, direccionamiento IP, entre otras.

Gate D es un programa dinámico que cambia al Omniswitch en un completo e integrado ambiente de ruteo. GateD soporta múltiples protocolos de enrutamiento, conjuntos de servicios (base datos de las tablas de enrutamiento y módulos de protocolos de enrutamiento). GateD es un ambiente de enrutamiento IP, conteniendo filtros, redistribución, adición y políticas de enrutamiento a través de los diferentes protocolos de enrutamiento con que cuenta el switch.

Entre algunas ventajas de la utilización de GateD se encuentran:

- La utilización de protocolos de enrutamiento como son RIP versión 1 y 2 y OSPF.
- Los beneficios de usar un programa que ha sido largamente probado en la industria como plataforma de enrutamiento.
- La opción a agregar nuevos protocolos de enrutamiento.
- La inclusión a los protocolos de enrutamiento de características como: "route preference", "route distribution", "route aggregation" y "routing policy enformcement"

El GateD realiza un enrutamiento dinámico, construyendo su propia base de datos de la información que es intercambiada entre los diferentes protocolos que están siendo utilizados en la red. GateD decide en cual ruta instalar la tabla de enrutamiento "kernel" y cuales comandos asignar. GateD también permite el

control de importar y exportar información de enrutamiento basado en protocolos, fuentes y destinos de sistemas autónomos, fuentes y destinos de interfaces, saltos del router y direcciones específicas de destino.

Puede especificar un nivel para cada combinación de información que se va a importar. Luego de asignar los niveles de preferencia, GateD realiza la decisión del cual ruta se va a utilizar, independientemente de los protocolos que están involucrados en la transferencia.

GateD no puede ser accesado directamente de la UI (user interface) del switch, aunque algunos de sus comandos de status y control si pueden ser desplegados . La razón de este diseño, es que GateD confía en los comandos utilizados en el archivo de configuración, el cual, se lee en el "boot" y le dice al switch las tareas por realizar. El archivo de configuración llamado *gated.conf*, contiene los comandos y parámetros utilizados para controlar las funciones de enrutamiento del switch. Entonces, para configurar el GateD, el programador debe crear estos archivos y cargarlos en el switch.

Entre los requerimientos de software y hardware se encuentran:

- 16 MB SIMM : necesario para cargar el sistema operativo y su propio funcionamiento (puede mantener hasta 15000 tablas de enrutamiento).
- Software de sistema operativo versión 3.0 o mayor.

5.2 Instalación y Configuración

Para configurar y cargar el nuevo programa (gated.conf) en el switch se deben seguir los siguientes pasos:

a. *Crear el archivo de configuración con el nombre gated.conf.:* Este archivo contiene los comandos y parámetros de configuración que definen al GateD su desempeño de enrutamiento en el switch. Sin una configuración válida, GateD no puede desempeñarse en su manera óptima. Para crear este archivo se puede utilizar cualquier programa de texto como "notepad" y luego de realizarlo se le cambia la extensión.

b. *Instalar el archivo en el switch*: para cargarlo simplemente se utiliza los programas FTP o ZMODEM. Una vez cargado el archivo es renombrado como gated.img.

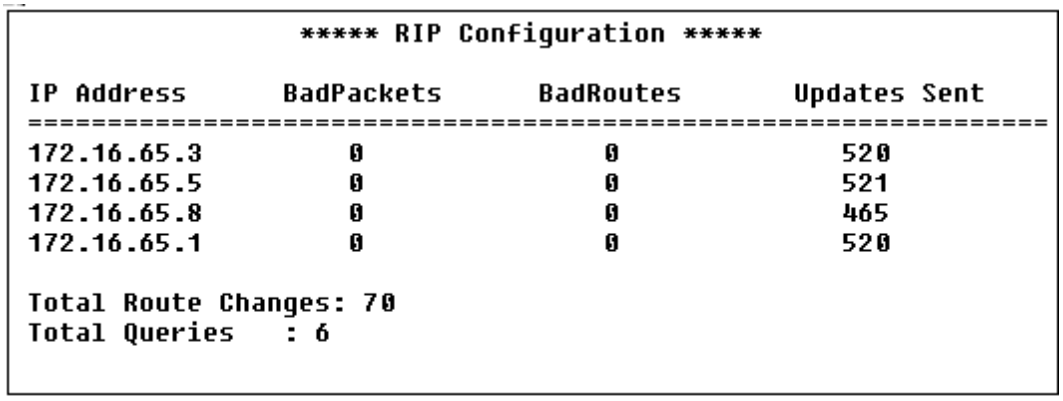
c. *"Reboot" (apagar y prender) el switch:* este procedimiento se realiza para que el nuevo archivo cargado empiece a trabajar. Una vez que el switch entre en funcionamiento, los comandos del UI aparecerán en el Menú de Redes (networking menu).

5.3 Comandos de la interfase de usuario (UI)

La interfase de usuario es orientada a comandos de raíz (root-command oriented), el cual significa que primero se debe ingresar la raíz del comando y este debe ser seguido por un subcomando o parámetro. Ingresar un comando de raíz sin ingresar un subcomando válido, produce un mensaje de error.

Los comandos utilizados para la interfase de usuario fueron:

- ***rip stat***: despliega información general acerca del desempeño del protocolo de enrutamiento RIP. Un ejemplo es el siguiente:

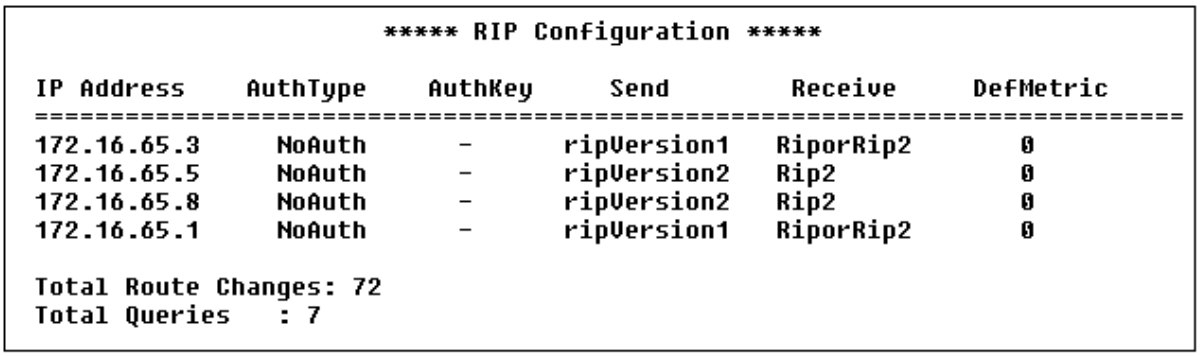


```
***** RIP Configuration *****

IP Address      BadPackets      BadRoutes       Updates Sent
================================================================
172.16.65.3          0               0              520
172.16.65.5          0               0              521
172.16.65.8          0               0              465
172.16.65.1          0               0              520

Total Route Changes: 70
Total Queries   : 6
```

Figura 5.1 Tabla desplegada por el comando *rip stat*

La figura 5.1 muestra las direcciones IP de las interfaces en la cual el protocolo RIP se encuentra y muestra también los paquetes malos recibidos, el número de rutas malas recibidas y el número enviado de actualizaciones en cada interfase.

- ***Rip conf:*** despliega la lista de interfaces que actualmente están configuradas para trabajar con RIP. Un ejemplo se muestra en la figura 5.2:



```
                    ***** RIP Configuration *****

IP Address    AuthType    AuthKey     Send        Receive     DefMetric
=============================================================================
172.16.65.3     NoAuth      -      ripVersion1   RiporRip2       0
172.16.65.5     NoAuth      -      ripVersion2   Rip2            0
172.16.65.8     NoAuth      -      ripVersion2   Rip2            0
172.16.65.1     NoAuth      -      ripVersion1   RiporRip2       0

Total Route Changes: 72
Total Queries   : 7
```

Figura 5.2 Tabla desplegada por el comando *rip conf*

El detalle de la figura 5.2 es el siguiente:

- IP Address: la dirección IP de la interfase
- Authentication Type (AuthType): es el tipo de autenticación utilizada por la interfase, pueden ser: no authentication, currently y only simple authentication.
- Send: este comando envía el tipo de interfase. Los valores pueden ser ripVersion1 y ripVersion2, rip1Compatible.
- Receive: este comando despliega el valor del tipo de interfase de donde viene. Los valores pueden ser: Rip1, Rip2 y Rip1orRip2.
- Default Metric (DefMetric): indica la métrica RIP utilizada por la interfase.

5.3 Sintaxis de Referencia del GateD

En esta sección se presentan los comandos del archivo de configuración gated.conf. Los comandos de configuración deben aparecer en un específico orden y se han clasificado en grupos, los cuales ayudan a definir su funcionalidad. Como precaución debe tenerse en cuenta que si se ingresa un comando fuera del orden establecido, lo más probable es que ocurra un error con excepción al "trace" el cual puede aparecer en cualquier parte.

La siguiente lista, muestra la clasificación por grupos de los comandos:

- **Grupo 1: *Options***
  Define las opciones globales, utiliza parámetros como :*nosend, noresolv, mark time y syslog.*

- **Grupo 2: *Interfaces***

Define e identifica las interfaces que se encuentran conectadas a la red. Una interfase es la conexión entre un router y la red, puede ser especificada por nombre, dirección IP o nombre del dominio.

- **Grupo 3: *Definition***

Comandos que identifican la configuración general del GateD con al menos un protocolo. Cuenta con los parámetros de identificación de *autonomous system* (sistema autónomo), *router ID configuration* (identificación de la configuración del router) y *martian configuration* (configuración de direcciones inválidas).

- **Grupo 4: *Protocol***

Comandos que establecen el protocolo de enrutamiento utilizado por el switch en la programación del GateD, entre ellos se encuentran: *rip* (habilita tanto a RIP1 como RIP2 o ambos), *OSPF, kernel* (configura las opciones de la interfase kernel).

- **Grupo 5: *Static***

Define las rutas estáticas que irán a ser utilizadas en el GateD. Un solo comando puede establecer varias rutas a la vez. Estas rutas pueden ser reescritas con rutas que contengan un valor de métrica mejor.

- **Grupo 6: *Control***

La política de rutas utilizada por el GateD representa un conjunto de reglas, las cuales, definen la relación entre el router y el mundo externo en relación a intercambios de rutas y la interacción de protocolos. Estas políticas actúan como filtros porque definen todo un conjunto filtros que se aplican a las rutas antes de aceptarlas o distribuirlas.

- **Grupo 7: *Aggregate***

Define el método de generar una ruta más general al tener una ruta específica. Se usa también en redes regionales o nacionales para reducir la cantidad de información de rutas que se da a través de esta. Con una programación adecuada las direcciones de clientes y redes regionales, pueden solamente anunciarse con una ruta de red regional en lugar de cientos de estas.

- **Grupo 8: *Trace***

Define la especificación de archivos, opciones de control, opciones globales y trazados de protocolos específicos.

CAPITULO 6

ANALISIS Y RESULTADOS

6.1 Explicación del diseño

6.1.1 Creación de perfiles de usuario

Lo primero que se hizo fue investigar al personal que trabaja en la SUGEF, donde se determinó en una primera instancia la cantidad y tipo de personal que trabaja en la entidad, esto con el objetivo de tener una idea de la carga que maneja cada switch por departamento. La figura 6.1 muestra la cantidad de personas por piso y su departamento:

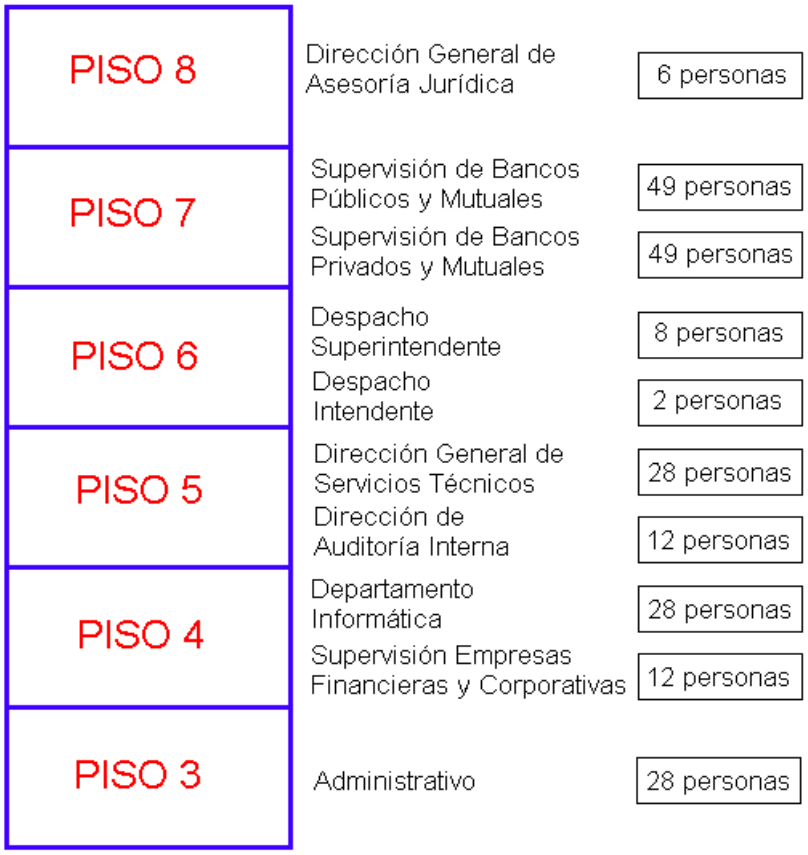


Figura 6.1 Cantidad de personal por piso en la SUGEF.

La figura 6.1 muestra la cantidad de personas que existen en la SUGEF por pisos, pero no indica nada de sus ocupaciones. Prácticamente la SUGEF, en su mayoría, los usuarios que tiene son supervisores o administradores, que se encargan de las entidades privadas y públicas del país. La figura 6.2 muestra como está distribuido el personal por perfiles de trabajo, donde con esta figura permite determinar las primeras conclusiones acerca de la creación de perfiles de usuario.

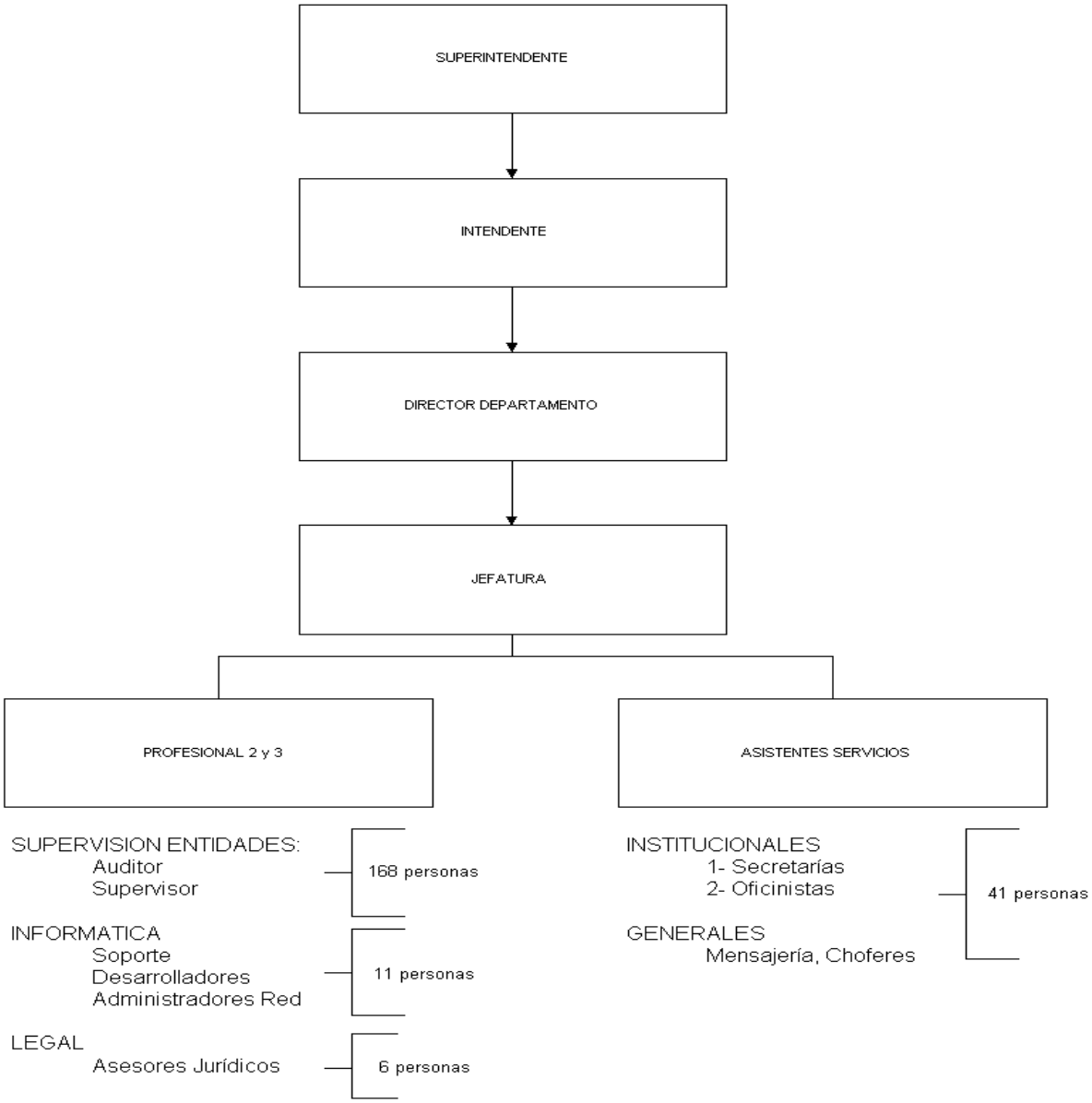


Figura 6.2 Distribución de personal para creación de perfiles

El siguiente paso que se realizó, una vez obtenido los perfiles de usuario, fue la investigación de la función que realiza cada servidor en la red. De acuerdo a este rol que cumplen, se hizo una división por grupos que a la vez sirve como diseño de VLAN, para diferenciar los grupos de trabajo que realiza cada servidor. Estos grupos son:

- **Grupo 1 (correspondencia):** Contiene a los servidores Faxination, Servidor de Correo y Correspondencia SUGEF.
- **Grupo 2 (aplicaciones):** Contiene solo al servidor de aplicaciones e impresión.
- **Grupo 3 (usuarios):** Contiene al servidor Intranet y portal.
- **Grupo 4 (olap):** Contiene a los servidores OLAP y Base Datos Producción. G
- **Grupo 5 (base datos):** contiene a los servidores Base Datos Desarrollo, SCA y respaldo.
- **Grupo 6 (administración):** contiene a los servidores Administración de Red, Radius y LSMS.
- **Grupo 7 (extranet):** contiene solo al servidor de extranet.

Los grupos de servidores están relacionados con los usuarios. Como todos los usuarios no tienen que utilizar todos los servidores, se crean perfiles de usuarios que se hicieron a partir del análisis de personal que anteriormente se mencionó. Los perfiles van a tener acceso a uno u otro servidor, dependiendo de la función que cumplen en la empresa.

De ahí se determinó los siguientes perfiles, en la figura 6.3:

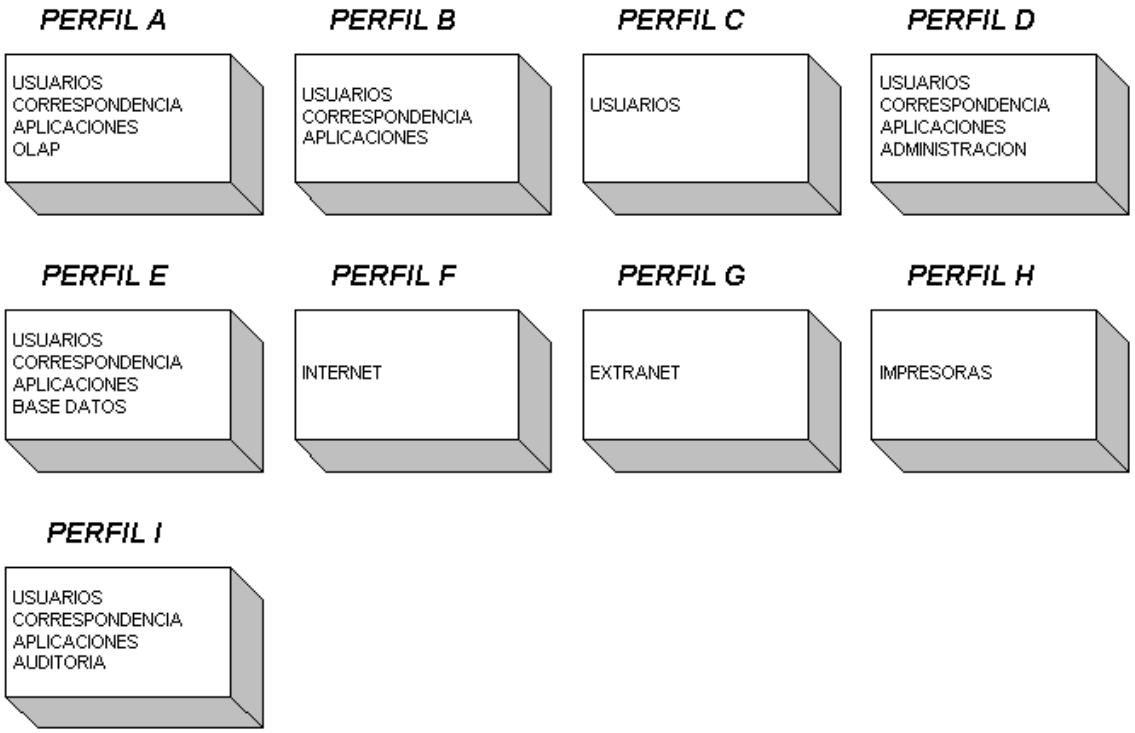


Figura 6.3 Diseño de perfiles de usuarios para la red de la SUGEF.

- **Perfil A:** es aplicado al usuario que se encarga de la supervisión de entidades financieras, es de propósito general y es la mayoría de personal que se encuentra en la SUGEF.
- **Perfil B:** es un perfil de propósito general. Es aplicado a personal temporal que se encuentra en la SUGEF y que no necesita acceso a ningún tipo de servicio específico.
- **Perfil C:** se utiliza para las salas de capacitación y microcomputadoras, donde personal que se va a capacitar solo necesitan el servidor de intranet para trabajar.
- **Perfil D:** es un perfil de propósito específico. Es aplicado a usuarios del departamento de informática y específicamente a aquellos que se encargan de la administración de la red.
- **Perfil E:** es un perfil de propósito específico. Es aplicado a usuarios del departamento de informática y específicamente a aquellos que se encargan del desarrollo de software aplicaciones en el servidor de producción.

- **Perfil F:** para usuarios externos a la entidad y que en un futuro se va a permitir el ingreso por internet.
- **Perfil G:** es un perfil de propósito general y aplicado a entidades bancarias financieras externas.
- **Perfil H:** es un perfil que agrupa a todas las impresoras que hay en la SUGEF, esto primero para llevar un control y segundo para establecer un tubo lógico para el flujo de tráfico de información.
- **Perfil I:** perfil de propósito específico y aplicado solo a los que trabajan en el departamento de auditoría.

6.1.2 Distribución de direcciones IP según servidores

El primer grupo de trabajo para el nuevo direccionamiento IP fue el de los servidores. Para el grupo de servidores se decidió tomar las direcciones 152.32.33.xx /27 y 152.32.34.xx /27.

Con estas dos direcciones se tomó, como política de diseño, "subnetear" en ocho grupos y que la primera y última subnet no se utilizara, para así separar el dominio de broadcast, permitiendo realizar un diseño óptimo en lo que respecta a cuellos de botella y mensajes que puedan colapsar a la red.

La tabla 6.1 es un resumen de lo que se mencionó anteriormente con respecto a la clasificación de los servidores, solo que ahora se le agregó a cada grupo un nombre, que identifica a un grupo de servidores.

Tabla 6.1 VLANs del grupo de servidores

NOMBRE VLAN	***SERVIDORES INCLUIDOS***
Usuarios	• Intranet • Portal
Correspondencia	• Servidor de Correo • Correspondencia SUGEF • Faxination
Aplica_Imprime	• Aplicaciones e Impresión
OLAP	• OLAP autoservicio • Base Datos Producción
Base Datos	• Base Datos Desarrollo • SCA • Respaldo
Administración	• Administrador de red (Adm-Net) • Radius • LSMS • Unix
Extranet	• Extranet

Ya con las políticas de diseño definida y los grupos hechos, se ajustó cada grupo de la tabla 6.1 a una subnet de las direcciones antes mencionadas. La tabla 6.2 muestra las direcciones asignadas a cada grupo de servidores.

Tabla 6.2 Grupo de direcciones IP asignadas al grupo de servidores

VLAN	SUBNET MASK	NETWORK NUMBER	IP INTERNAL ROUTER	BROADCAST ADDRESS
Usuarios	255.255.255.224	152.32.33.32	152.32.33.33	152.32.33.63
Correspondencia	255.255.255.224	152.32.33.64	152.32.33.65	152.32.33.95
Aplica_Imprime	255.255.255.224	152.32.33.96	152.32.33.97	152.32.33.127
OLAP	255.255.255.224	152.32.33.128	152.32.33.129	152.32.33.159
Base Datos	255.255.255.224	152.32.33.160	152.32.33.161	152.32.33.191
Administración	255.255.255.224	152.32.33.192	152.32.33.193	152.32.33.223
Extranet	255.255.255.224	152.32.34.32	152.32.34.33	152.32.34.63

Con los grupos definidos, la dirección antigua de los servidores necesita actualizarse a aquella que se ajusta al grupo en que fue asignada cada servidor. La tabla 6.3 muestra las nuevas direcciones IP que fueron asignadas.

Como no todas las direcciones fueron ocupadas, la tabla 6.4 muestra las direcciones disponibles que tiene el administrador para realizar en un futuro si se presenta, la adición de nuevo equipo a la red, siempre que se ajuste al grupo y perfil que fueron definidos.

Tabla 6.3 Asignación de las direcciones IP de cada servidores según VLAN

VLAN	SERVIDOR	DIRECCION IP
Usuarios	Intranet	152.32.33.34
	Portal	152.32.33.35
Correspondencia	Servidor de Correo	152.32.33.66
	Correspondencia SUGEF	152.32.33.67
	Faxination	152.32.33.68
Aplica_Imprime	Aplicaciones e Impresión	152.32.33.98
OLAP	OLAP Autoservicio	152.32.33.130
	Base Datos Producción	152.32.33.131
Base Datos	Base Datos Desarrollo	152.32.33.162
	SCA	152.32.33.163
	Respaldo	152.32.33.164
Administración	Administrador de red	152.32.33.194
	Radius	152.32.33.195
	Unix	152.32.33.196
	LSMS	152.32.33.197
Extranet	Extranet	152.32.34.34

Tabla 6.4 Direcciones IP válidas para servidores según VLAN

VLAN	DIRECCIONES IP (DESDE - HASTA) (1)		HOST
Usuarios	152.32.33.36	152.32.33.62	27
Correspondencia	152.32.33.69	152.32.33.94	26
Aplica_Imprime	152.32.33.100	152.32.33.126	28
OLAP	152.32.33.132	152.32.33.158	27
Base Datos	152.32.33.165	152.32.33.190	25
Administración	152.32.33.198	152.32.33.222	25
Extranet	152.32.34.35	152.32.34.62	28

(1) Todas las direcciones son inclusive

La figura 6.4 muestra un resumen de lo realizado anteriormente. La primera y última subnet de cada dirección (33 y 34) por criterios de diseño se reservan, además quedó 4 grupos de direcciones no asignados previniendo a un futuro de que se deseara ingresar un servidor que no aplica dentro de los grupos ya formados.

	Network Number
RESERVADA	152.32.33.224
ADMINISTRACION	152.32.33.192
BASE DATOS	152.32.33.160
OLAP	152.32.33.128
APLICA_IMPRIME	152.32.33.96
CORRESPONDENCIA	152.32.33.64
USUARIOS	152.32.33.32
RESERVADA	152.32.33.0

	Network Number
RESERVADA	152.32.34.224
NO ASIGNADO 4	152.32.34.192
NO ASIGNADO 3	152.32.34.160
NO ASIGNADO 2	152.32.34.128
NO ASIGNADO 1	152.32.34.96
SWITCHES	152.32.34.64
EXTRANET	152.32.34.32
RESERVADA	152.32.34.0

Figura 6.4 Mapeo del direccionamiento IP 33 y 34

6.1.3 Distribución de direcciones IP según perfiles de usuario

Para los perfiles de usuario se han asignado las direcciones 152.32.35.xx /27, 152.32.36.xx /27, 152.32.36.xx /27, con las mismas políticas de diseño del punto anterior.

Al igual que se hizo en el apartado anterior, la tabla 6.5 muestra un resumen de los perfiles creados y a que grupo de servidores pueden tener acceso. Para simplificar un poco más el proceso de identificación, se decidió colocar el nombre que va de perfil A hasta perfil I.

La tabla 6.6 siguiendo con la metodología del punto anterior, determina la asignación de grupos de direcciones IP de acuerdo al perfil Para determinar cuantos grupos de subnets es necesario asignarle a cada perfil, la decisión se tomó por medio de la figura 6.2, en donde dependiendo de la cantidad de usuarios que tenga así se trató de que existiera un número por lo menos igual. En todos los casos se dejó un numero superior de hots para así, prever en un futuro cualquier nuevo ingreso de usuarios.

Tabla 6.5 VLANs del grupo de perfiles de usuario con acceso a servidores

NOMBRE VLAN	ACCESO A VLAN-GRUPO SERVIDORES
Perfil A (personal de supervisión entidades)	• Usuarios • Correspondencia • Aplicaciones • OLAP
Perfil B (personal temporal)	• Correspondencia • Aplicaciones
Perfil C (capacitación de personal)	• Usuarios
Perfil D (informática - administración de la red)	• Usuarios • Correspondencia • Aplicaciones • Administración
Perfil E (informática - base datos desarrollo, producción y respaldos)	• Usuarios • Correspondencia • Aplicaciones • Base Datos
Perfil F (internet)	• Internet
Perfil G (usuarios externos)	• Extranet
Perfil H (impresoras del edificio)	• Aplica_Imprime
Perfil I (solo para personal de auditoría)	• Usuarios • Correspondencia • Aplicaciones • Auditoría

Tabla 6.6 Grupo de direcciones IP asignadas al grupo de perfiles

VLAN	Subnet Mask	Network Number	Broadcast Address	Number of IP Address
Perfil A.1	255.255.255.224	152.32.35.32	152.32.35.63	30
Perfil A.2	255.255.255.224	152.32.35.64	152.32.35.95	30
Perfil A.3	255.255.255.224	152.32.35.96	152.32.35.127	30
Perfil A.4	255.255.255.224	152.32.35.128	152.32.35.159	30
Perfil A.5	255.255.255.224	152.32.35.160	152.32.35.191	30
Perfil A.6	255.255.255.224	152.32.35.192	152.32.35.223	30
Perfil B	255.255.255.224	152.32.36.32	152.32.36.63	30
Perfil C	255.255.255.224	152.32.36.64	152.32.36.95	30
Perfil D	255.255.255.224	152.32.36.96	152.32.36.127	30
Perfil E	255.255.255.224	152.32.36.128	152.32.36.159	30
Perfil F	255.255.255.224	152.32.36.160	152.32.36.191	30
Perfil G.1	255.255.255.224	152.32.36.192	152.32.36.223	30
Perfil G.2	255.255.255.224	152.32.37.32	152.32.37.63	30
Perfil H.1	255.255.255.224	152.32.37.64	152.32.37.95	30
Perfil H.2	255.255.255.224	152.32.37.96	152.32.37.127	30
Perfil I.1	255.255.255.224	152.32.37.128	152.32.37.159	30
Perfil I.2	255.255.255.224	152.32.37.160	152.32.37.191	30

La tabla 6.7 muestra la cantidad total de usuarios que puede tener cada perfil, según el estudio que se había hecho anteriormente. Como se mencionó, cada perfil tiene un número mayor al que se encuentran laborando actualmente en la SUGEF.

Tabla 6.7 Cantidad total de usuarios por perfil

VLAN	CANTIDAD DE HOST
Perfil A (personal de supervisión entidades)	180
Perfil B (personal temporal)	30
Perfil C (capacitación de personal)	30
Perfil D (informática - administración de la red)	30
Perfil E (informática - base datos y respaldo)	30
Perfil F (internet)	30
Perfil G (usuarios externos - extranet)	60
Perfil H (impresoras del edificio)	60
Perfil I (solo para personal de auditoría)	60

Un resumen de la distribución de direcciones IP, se presenta en la figura 6.5, donde muestra que solo puede crearse un nuevo perfil de usuario; si alguno de ellos no se ajusta a un nuevo tipo de trabajador que ingrese a la SUGEF o que por algún motivo alguno de los perfiles llegue a llenarse.

	Network Number
RESERVADA	152.32.35.224
PERFIL A.6	152.32.35.192
PERFIL A.5	152.32.35.160
PERFIL A.4	152.32.35.128
PERFIL A.3	152.32.35.96
PERFIL A.2	152.32.35.64
PERFIL A.1	152.32.35.32
RESERVADA	152.32.35.0

	Network Number
RESERVADA	152.32.36.224
PERFIL G.1	152.32.36.192
PERFIL F	152.32.36.160
PERFIL E	152.32.36.128
PERFIL D	152.32.36.96
PERFIL C	152.32.36.64
PERFIL B	152.32.36.32
RESERVADA	152.32.36.0

	Network Number
RESERVADA	152.32.37.224
NO ASIGNADO 1	152.32.37.192
PERFIL I.2	152.32.37.160
PERFIL I.1	152.32.37.128
PERFIL H.2	152.32.37.96
PERFIL H.1	152.32.37.64
PERFIL G.2	152.32.37.32
RESERVADA	152.32.37.0

Figura 6.5 Mapeo del direccionamiento IP 35 , 36 y 37

Más adelante en los diseños de las VLAN, se va a mostrar que dentro de cada perfil que se ha formado, se debe reservar 6 direcciones IP, esto debido a que a este diseño como es el mismo para cada piso, se necesita sacrificar direcciones IP. Por lo tanto, la tabla 6.8 muestra el grupo de direcciones válidas, que el administrador va a poder utilizar para asignar a usuarios.

Tabla 6.8 Direcciones válidas para usuarios según perfil

VLAN	DIRECCIONES IP (DESDE - HASTA) (1)		HOST
Perfil A.1	152.32.35.39	152.32.35.62	24
Perfil A.2	152.32.35.71	152.32.35.94	24
Perfil A.3	152.32.35.103	152.32.35.126	24
Perfil A.4	152.32.35.135	152.32.35.158	24
Perfil A.5	152.32.35.167	152.32.35.190	24
Perfil A.6	152.32.35.199	152.32.35.222	24
Perfil B	152.32.36.39	152.32.36.62	24
Perfil C	152.32.36.71	152.32.36.94	24
Perfil D	152.32.36.103	152.32.36.126	24
Perfil E	152.32.36.135	152.32.36.158	24
Perfil F	152.32.36.167	152.32.36.190	24
Perfil G.1	152.32.36.199	152.32.36.222	24
Perfil G.2	152.32.37.39	152.32.37.62	24
Perfil H.1	152.32.37.71	152.32.37.94	24
Perfil H.2	152.32.37.103	152.32.37.126	24
Perfil I.1	152.32.37.135	152.32.37.158	24
Perfil I.2	152.32.37.167	152.32.37.190	24

(1) Todas las direcciones son inclusive.

6.1.4 Diseño de VLAN

El diseño de las VLAN, consta de dos partes. Primero, un diseño de la VLAN del switch principal (figura 6.6), donde muestra el grupo de servidores, cada uno con su respectiva dirección IP hacia un router interno que se programa internamente en las VLAN. Existe también un grupo de "backbone", donde este grupo es la unión lógica ente un switch departamental y el switch principal, esto con el objetivo de que las VLANs entre switches no se vean separadas, sino que todo el conjunto de switches existentes en la red se vea todo como un solo.

Estas políticas se definieron de acuerdo al manual de usuario del switch y es la característica principal para la formación de grupos de VLAN entre switches para los Xylan.

Con respecto al diseño de las VLAN departamentales (figuras 6.7 a la figura 6.9), prácticamente el mismo diseño que se realiza para cualquier piso de los Omnistack se mantiene para todos los pisos, lo que varía es la dirección IP del router interno. Este diseño se realizó así con el fin de que sea un sistema versátil, es decir, no importa de adonde ingrese el usuario, que siempre va a estar en el mismo perfil. Con ello nos aseguramos que si existe algún movimiento de personal entre pisos o departamentos, el cambio sea totalmente transparente, sin modificaciones de software o de hardware. Para que este sistema trabaje bien, se debe asignar una política de direcciones MAC entre los switches, es decir, cuando se vaya a realizar la migración, según el plan que más adelante se presenta, a cada switch de la red, hay que programarle las direcciones MAC, esto con el fin de asegurar que el usuario entre correctamente a su VLAN y también brindar seguridad ante computadoras que no estén autorizada a entrar en la red de la SUGEF.

Las siguientes figuras muestran gráficamente lo que se ha explicado en los párrafos anteriores.

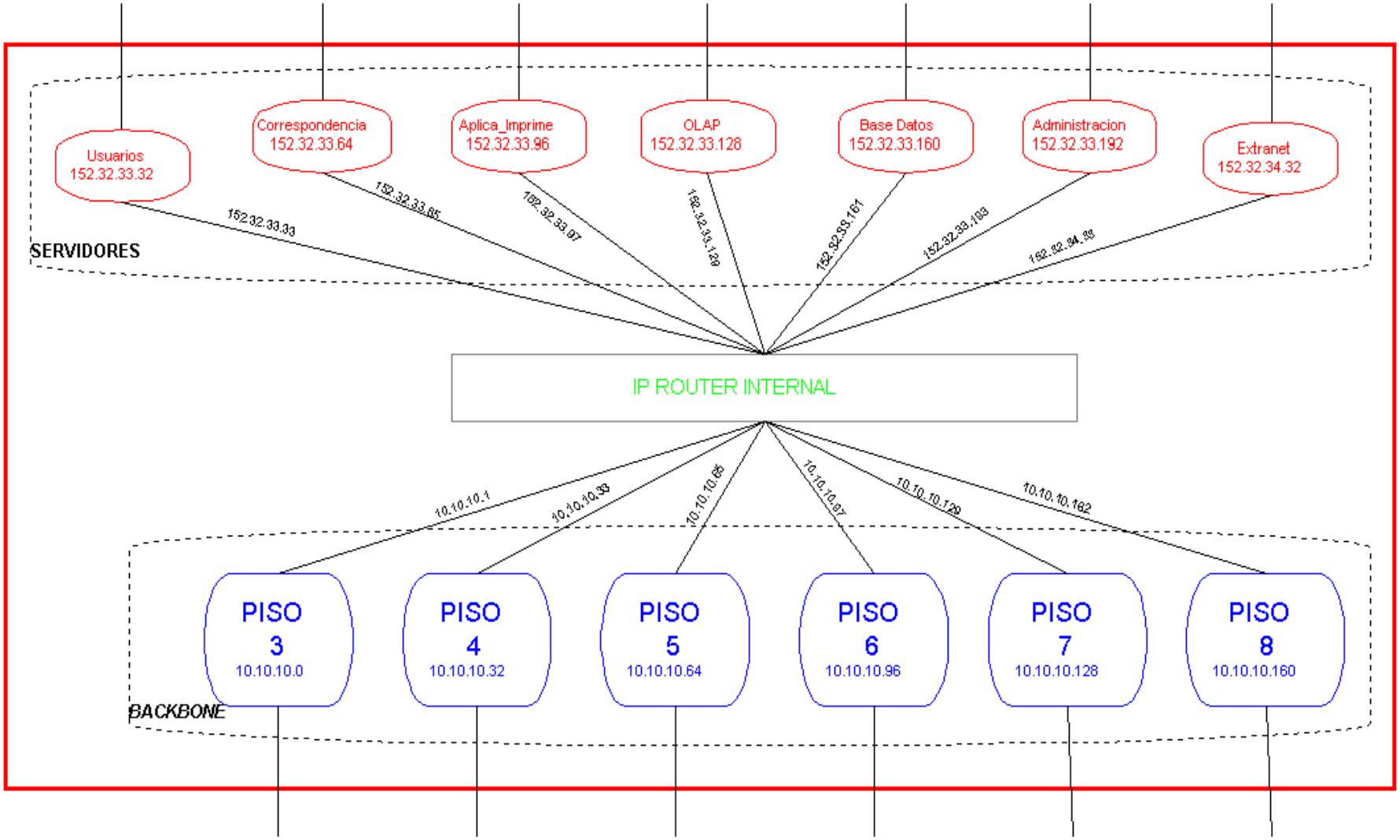


Figura 6.6 Diseño de VLAN switch principal

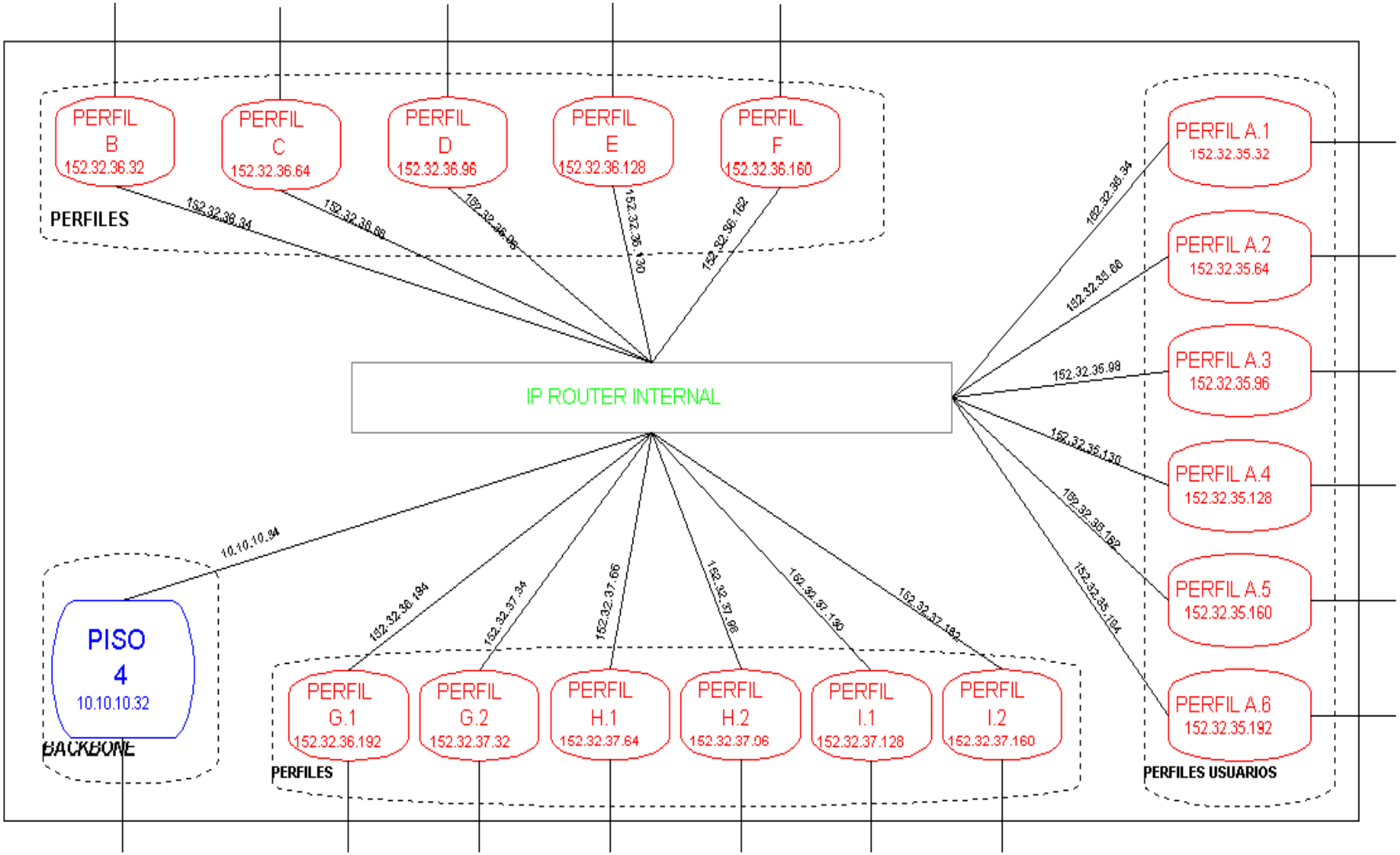


Figura 6.7 Diseño VLAN piso 4

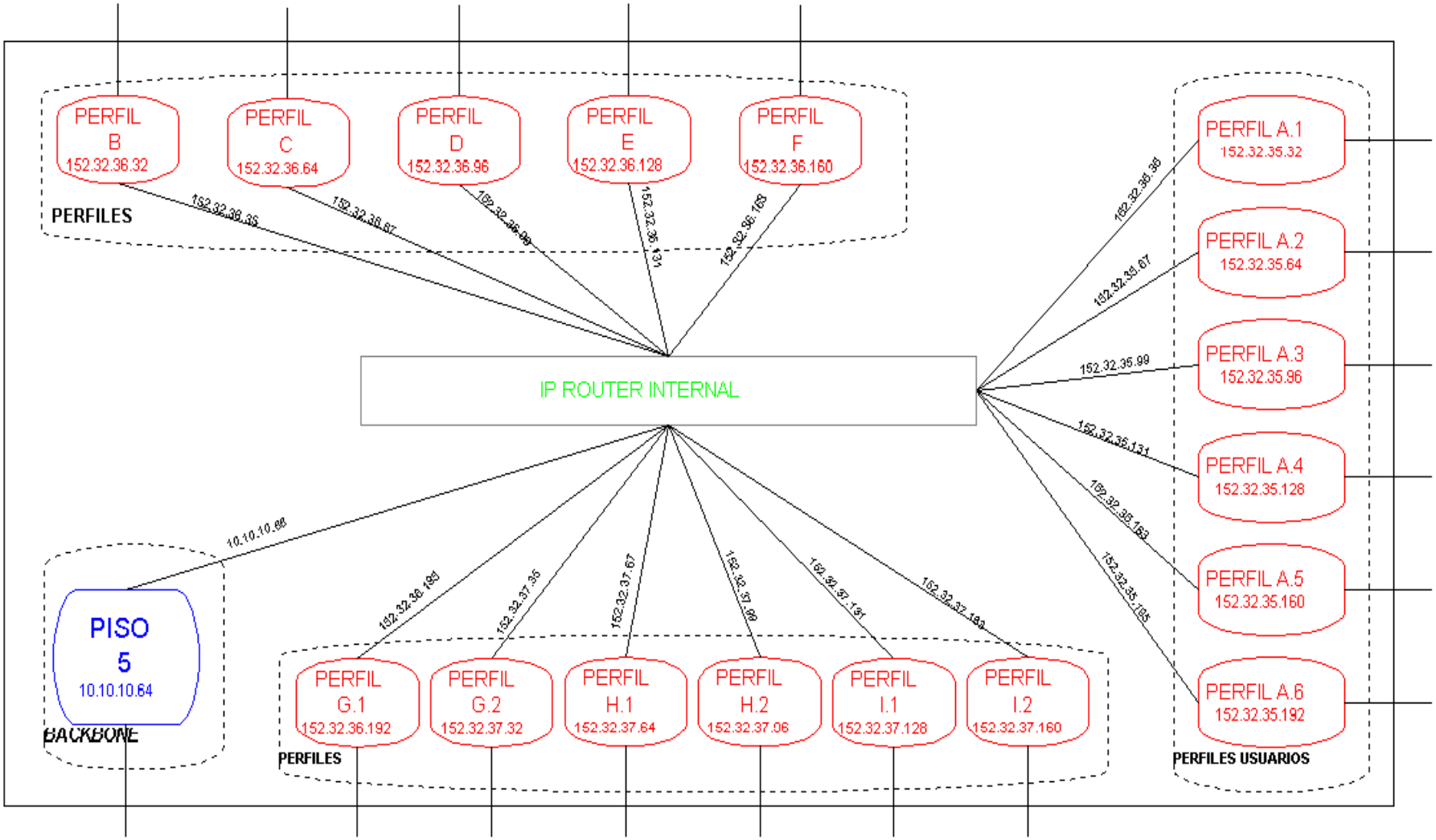


Figura 6.8 Diseño VLAN piso 5

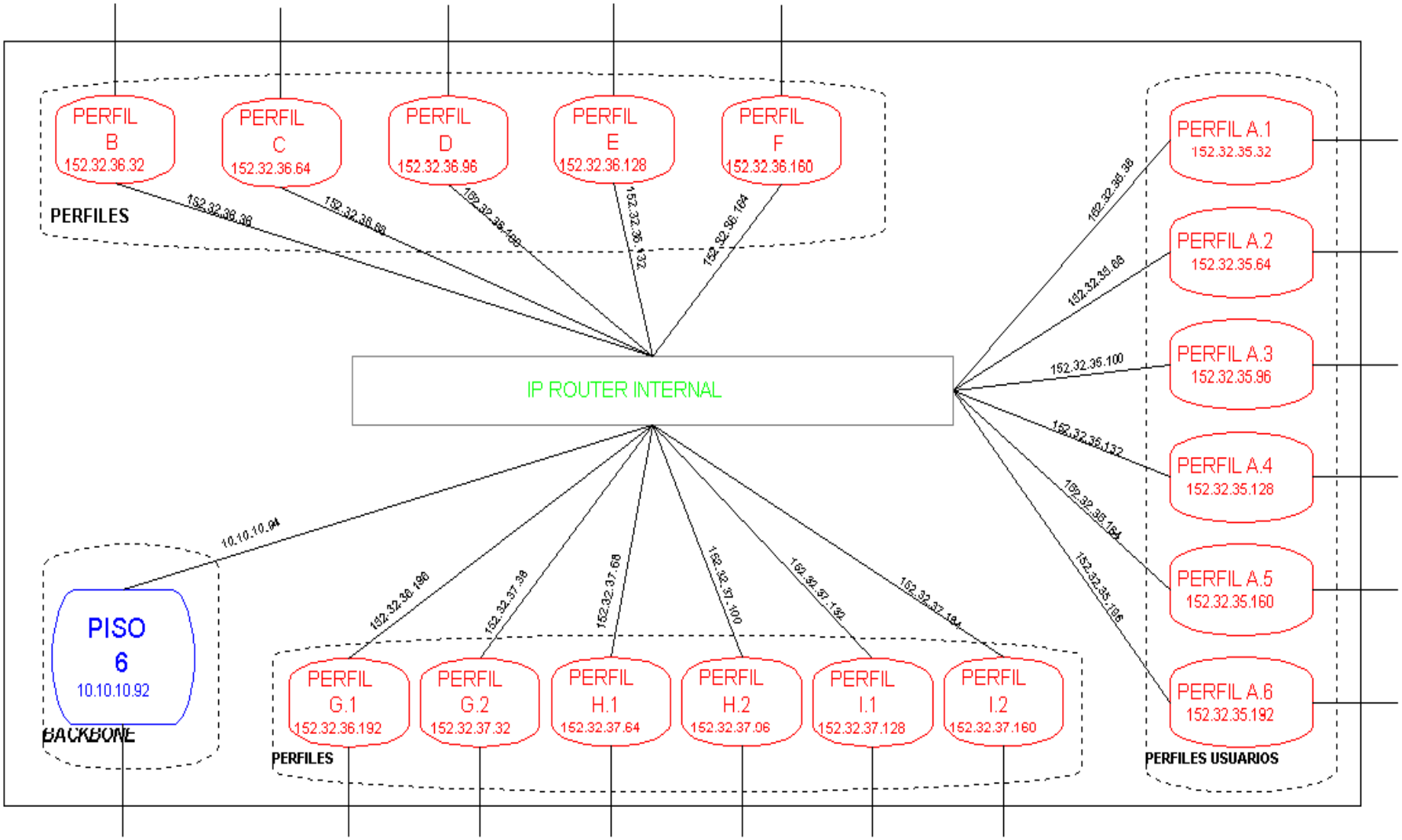


Figura 6.9 Diseño VLAN piso 6

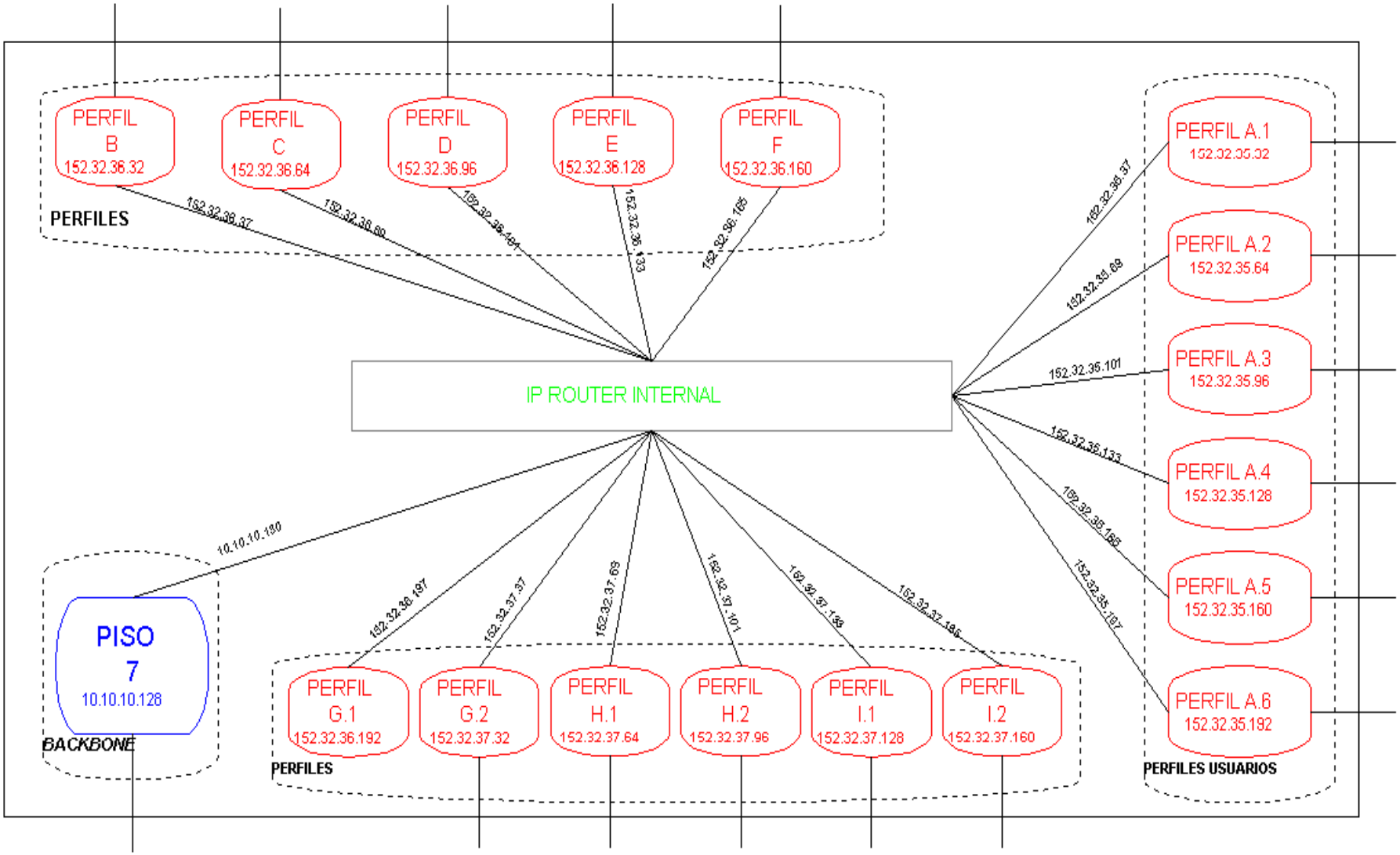


Figura 6.10 Diseño VLAN piso 7

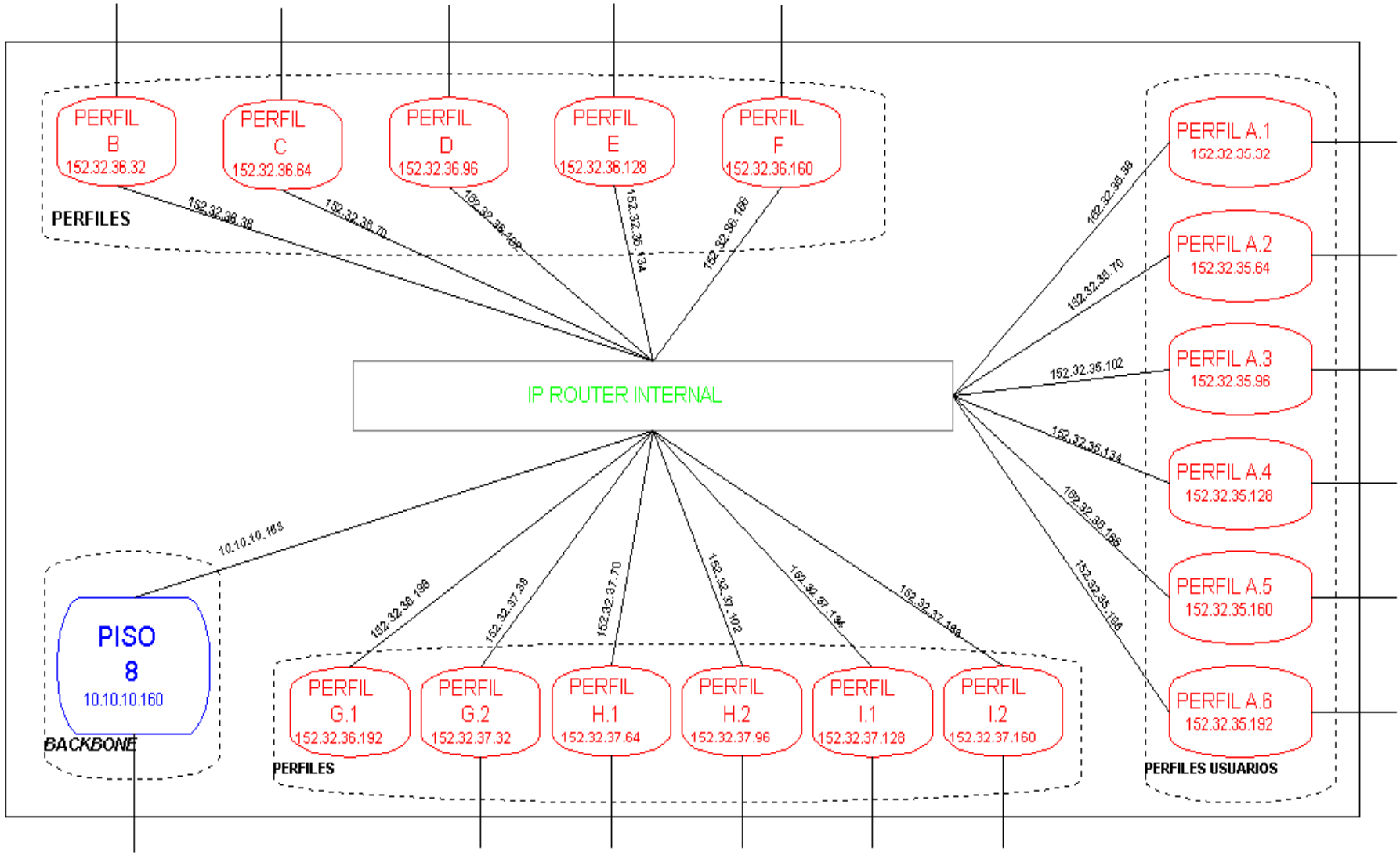


Figura 6.11 Diseño VLAN piso 8

6.1.5 Escogencia del protocolo de enrutamiento

De acuerdo a la literatura consultada y experiencias de otras personas en instituciones, se determinaron las características más importantes de cada protocolo. Este análisis concluyó con una justificación del porqué en este momento es mejor la utilización del protocolo de enrutamiento RIP v2. En el apéndice 3, 4 y 5 hay mayor información relacionada con estos tres tipos de protocolos de enrutamiento.

a.- Características RIP 1

- El número de saltos es el número de dispositivos que deben atravesar para llegar hasta la red deseada. RIP tiene un máximo de 15 saltos; por tanto, sólo puede haber 15 dispositivos entre dos hosts cualesquiera

- RIP permite la existencia de múltiples entradas en la tabla de enrutamiento de una red si hay múltiples rutas de acceso. El proceso de enrutamiento IP elige la ruta con la medida menor (menos saltos) como la mejor ruta

- Puesto que sólo se pueden enviar 25 rutas en un único paquete RIP, las tablas de enrutamiento grandes tienen que enviarse como múltiples paquetes RIP.

- Los enrutadores RIP anuncian el contenido de sus tablas de enrutamiento cada 30 segundos en todas las redes conectadas mediante una subred IP y difusión de nivel MAC

- RIP v1 se diseñó para satisfacer las necesidades de enrutamiento dinámico de las redes IP basadas en tecnología LAN. Las tecnologías LAN de acceso compartido, como Ethernet y Token Ring, admiten difusión de nivel MAC (Control de acceso a medios), donde varios nodos de la red pueden recibir y procesar un único paquete. Sin embargo, en las redes modernas, el uso de

difusiones de nivel MAC no es deseable ya que todos los nodos deben procesar todas las difusiones.

- RIP v1 se diseñó para las redes IP basadas en clases, donde el Id. de red puede determinarse a partir de los valores de los 3 primeros bits de la dirección IP de la ruta RIP. Como la máscara de subred no se incluye con la ruta, el enrutador RIP debe determinar el Id. de red basándose en un conjunto limitado de información.

- El Id. de red basada en clases sólo se anuncia fuera del entorno con subredes, las subredes de un Id. de red en un entorno RIP v1 deben ser contiguas. Si las subredes de un Id. de red IP no son contiguas, lo que se denomina subredes disjuntas, enrutadores RIP v1 independientes anuncian en distintas partes de la red el Id. de red basada en clases. Como resultado de ello, es posible reenviar el tráfico IP a la red incorrecta.

- RIP v1 no proporciona ninguna protección para evitar que un enrutador RIP con intenciones ingresar en la red ingrese y anuncie rutas erróneas o imprecisas. Los anuncios RIP v1 se procesan independientemente de cuál sea su origen. Un usuario malintencionado podría utilizar esta falta de protección para sobrecargar los enrutadores RIP con cientos o miles de rutas incorrectas o imprecisas.

b.- Características RIP 2

- En vez de difundir anuncios RIP, RIP v2 admite el envío de anuncios RIP a la dirección de multicast IP 224.0.0.9. Los nodos que no son RIP no se ven afectados por el tráfico de anuncios de los enrutadores RIP.

- Los anuncios RIP v2 envían la máscara de subred junto con el Id. de red. Se puede utilizar RIP v2 en entornos de subredes, de superredes y de máscara

de subred de longitud variable. Las subredes de un Id. de red no tienen que ser contiguas (pueden ser subredes disjuntas).

- RIP v2 admite el uso de mecanismos de autenticación para comprobar el origen de los anuncios RIP entrantes. En RFC 1723 se definió la autenticación por clave de acceso simple, pero existen mecanismos de autenticación más recientes, como Message Digest 5 (MD5, Síntesis del mensaje 5).

- Para asegurar que los enrutadores RIP v1 pueden procesar anuncios RIP v2, RIP v2 no modifica la estructura del formato de mensajes RIP. RIP v2 utiliza los campos que en RIP v1 se definieron como Debe ser cero.

- Permite algoritmos de convergencia de horizonte dividido, rutas inalcanzables y actualizaciones desencadenadas.

- RIP v2 tiene la capacidad para modificar el intervalo de anuncio (el valor predeterminado es de 30 segundos) y la capacidad para modificar el valor de tiempo de espera de las entradas de la tabla de enrutamiento (el valor predeterminado es de 3 minutos).

- RIP v2 también tiene la capacidad de filtrado de un mismo nivel, o sea, la posibilidad de aceptar o descartar actualizaciones de anuncios procedentes de determinados enrutadores identificados por dirección IP.

- Posibilidad de difundir (como unicast) anuncios RIP a enrutadores específicos para admitir tecnologías de no difusión como Frame Relay. Un vecino RIP es un enrutador RIP que recibe anuncios RIP por unicast.

c.- Características OSPF

- OSPF puede detectar y propagar los cambios de topología más rápido que RIP. La cuenta hasta el infinito no se produce con OSPF.

- Las rutas calculadas (link-state) se basan en costos de saltos y anchos de banda, escogiendo la que mejor se presente y nunca tienen loops

- Con OSPF, un sistema autónomo puede subdividirse en grupos contiguos de redes denominados áreas. Es posible resumir las rutas dentro de las áreas para reducir al mínimo las entradas de la tabla de rutas. Las áreas pueden configurarse con una ruta predeterminada que resuma todas las rutas externas al sistema autónomo o al área.

- OSPF puede adaptarse a redes grandes y muy grandes.

- OSPF permite la carga balanceada.

- OSPF envía tablas de enrutamiento solo si ocurre un cambio en la red, esto asegura un mejor aprovechamiento del ancho de banda.

- OSPF se diseñó para anunciar la máscara de subred con la red. OSPF admite máscaras de subred de longitud variable (VLSM), subredes disjuntas y superredes.

- Se pueden autenticar los intercambios de información entre rutas OSPF. Admite autenticación por clave de acceso simple.

- Las rutas externas al sistema autónomo de OSPF se anuncian dentro del sistema autónomo, por lo que los enrutadores OSPF pueden calcular la ruta de menor costo a las redes externas.

d.- Justificación de la escogencia del protocolo de enrutamiento

El protocolo escogido luego de realizar un análisis de la red y los dos protocolos de enrutamientos escogidos, se definió que se ajustaba mejor el protocolo RIP en su versión 2.

Se analizó aspectos como:

- El número de saltos que tenía que hacer la red que no es más de dos en cualquier nodo de transmisión de información.
- Ambos protocolos pueden realizar subneteos, multicast, unicast.
- OSPF se diseño para WAN y LAN de gran tamaño donde manejan un gran número de tablas de enrutamiento en comparación con el RIP v2 que fue diseñado específicamente a redes pequeñas y medianas.
- Por saturamiento del ancho de banda de la red o por el envío constante de tablas de enrutamiento se hizo el siguiente cálculo para ejemplificar:

  De acuerdo al diseño de la reestructuración de la red, que se puede notar en la figura 6.4 y 6.5 **,** se determinó que la red propuesta tendría aproximadamente 28 subredes, que esto implica que se tendrían que enviar 2 paquetes que contienen las tablas de enrutamiento. Cada paquete tiene un tamaño máximo de 504 bytes o sea que dos paquetes, suponiendo con 50 rutas o subredes, tendría un tamaño de 1 Kb. Todos los enlaces son de 155 Mbs entre switches, por lo que la carga de envío de tablas de enrutamiento entre switches es despreciable, por lo que este se descartó como argumento de peso, al compararlo con el protocolo de enrutamiento OSPF.

  El tamaño de los paquetes que envía RIP v2 en compración con OSPF, se nota una gran diferencia, porque otro cálculo igual que el anterior determinó que un paquete con 50 rutas en OSPF tiene un tamaño de 150 bytes y las actualizaciones pueden ser menores de 75 bytes.

- RIP v2 es fácil de implementar, es tan sencillo como configurar direcciones IP y máscaras de subred para cada interfaz del switch. Esto es una gran ventaja sobre el OSPF, debido a que la red de la SUGEF necesita realizar o implementar esta migración de forma rápida, con el menor trabajo posible y asegurándose que esta migración sea estable en su funcionamiento y no haya que estar haciéndole "patches" para evitar así problemas con los usuarios internos y externos.

- RIP v2 tiene una gran base instalada que consta de redes IP de tamaño pequeño o medio que no desean afrontar la carga del diseño y la configuración de OSPF.

- También esta decisión se apoyó en una tesis "Protocols and Computer Networks" del Dr. Debby Koren de la Tel-Aviv University que menciona en una parte de su documento y realizando la traducción lo más fiel posible "…..cuando una red es pequeña, existe conexiones punto a punto entre dispositivos y no existen rutas redundantes, el ruteo estático (stactic routing) es suficiente. Pero si uno de estas tres condiciones es falsa, el ruteo dinámico (dynamic routing) es normalmente usado." Se conoce como protocolos "static routing" a las versiones 1 y 2 de RIP y los "dynamic routing" como por ejemplo el protocolo OSPF. Se mencionó anteriormente la red de la SUGEF claramente tiene las características que menciona el Dr. Koren por lo que se tomó este como aspecto determinante para la escogencia de RIP v2.

6.1.5 Plan de Migración

a.- Consideraciones DHCP

Para lograr definir y conocer las características de las asignaciones de direcciones dinámicas, se realizó un estudio y el Apéndice 6 muestra un documento que abarca las consideraciones DHCP. Lo siguiente son las características más importantes para lograr utilizar este parámetro en la reestructuración de la red.

Se va a definir primero los problemas de utilizar direcciones estáticas en una red:

- No utiliza eficientemente las direcciones asignadas
- No es segura contra la duplicación
- No facilita movilidad
- Complicado para moverse, agregar y cambiar direcciones.
- No ofrece información de uso
- No hay autenticación.
- Ingreso manual de dirección IP, gateway, DNS, WINS y dominio.

En cambio al utilizar DCHP en una red se pueden tener las siguientes ventajas:

- Usuarios están disponibles a conectar sus nuevas máquinas a la red automáticamente y reciben su dirección IP, gateway, DNS, WINS y dominio por defecto.
- Ayuda a prevenir la duplicación de direcciones.
- Eficiente uso del dominio IP.
- Previene errores en la configuración
- Permite la configuración de una gran cantidad de dispositivos en una corta cantidad de tiempo.
- La oficina, departamento, usuario puede moverse transparentemente.

- Facilita la administración de direcciones IP.
- Permite la autenticación vía registro de direcciones MAC.
- Clientes en áreas públicas, cuartos de conferencia o cuartos de estudios con una dirección MAC registrada pueden obtener una dirección IP.

Para lograr una solución con estas características se debe cumplir con las siguientes condiciones:

- Autenticar clientes utilizando direcciones MAC.
- DNS dinámico para clientes con DHCP
- Respaldo DHCP

También se debe cumplir con una serie de políticas de red para cumplir con el uso eficiente del DCHP:

- Todos los clientes DHCP deben tener una dirección MAC registrada.
- Direcciones permanentes serán dadas a impresoras y servidores.
- La persona que utiliza la computadora debe ser responsable del registro de la dirección MAC.
- Todas las direcciones MAC expirarán a un año y para renovarla debe cumplir que sea notificada vía e-mail.

b.- Diferencias entre DHCP y VLAN

Los conceptos DHCP y VLAN son muy diferentes, pero muchas veces son nombrados para resolver un mismo problema. Mientras ellos tienen un objetivo en común (facilidad de movimiento de las computadoras en la red), las VLAN representa un cambio más revolucionario que DHCP en LAN. Un servidor de DHCP permite desconectar a un cliente de una red o subnet y conectarla en otra, sin mayores problemas porque esta reconfiguración se hace automática. También en conjunto con el DNS, el DCHP puede dar nombres de diferentes dominios según se establezca por el administrador.

Por otro lado las VLAN permite a los clientes conectarse de diferentes puertos y tener la misma dirección IP y estar en la misma subnet. También las VLAN tienen políticas de configuración de listas de direcciones MAC que permiten ingresar a VLAN definidas anteriormente por el administrador.

Algunas diferencias entre DCHP y VLAN son:

- DCHP maneja cambios de reconfiguración del cliente, mientras que la VLAN maneja cambios de reconfiguración si el cliente ha sido movido del puerto en que se encontraba.
- DCHP requiere un servidor, mientras que las VLAN requiere que todos los hubs y equipo que está a través de la red sean capaz de soportar el esquema diseñado.
- DHCP puede configurar a un nuevo cliente, mientras que las VLAN no pueden.
- DHCP es capaz de realizar "movimientos fáciles" a través de redes que han sido divididas en subnets, geográficamente o redes separadas totalmente. VLAN solo permite realizar subnets en una misma área.

c.- Plan de Acción

1.- Switches

- **Cambio de protocolo de enrutamiento**

Se debe realizar la migración del protocolo de enrutamiento RIP v.1 a RIP v.2 realizando esta tarea paralelamente en todos los switches de la red. La ventaja que existe, es que la programación realizada para un switch va a ser la misma para los otros switches de cada departamento.

- **Pruebas y estabilidad de la red**

Luego de realizar la migración se debe dejar un tiempo de análisis y comportamiento de la red ante el nuevo cambio que se le realizó. Se recomienda que se monitoree la red por lo menos una semana, ante cualquier problema que

se pueda presentar y no realizar ningún otro paso hasta estar seguro que la migración fue realizada con éxito.

- **Creación de nuevas VLAN**

Como parte de la reestructuración de la red implica realizar un redireccionamiento IP, se deben crear las VLAN que cumplan con las políticas de este nuevo redireccionamiento y que se mencionó anteriormente en la propuesta de red.

Como las direcciones 152.32.33.xx/24 y 152.32.34.xx/24 están siendo utilizadas en la red, estas direcciones todavía no van a ser modificadas y van a mantener la estructura actual de VLAN.

En esta primera etapa de creación de VLAN solo se van a crear las nuevas VLAN con las políticas antes definidas en las direcciones 152.32.35.xx/27 , 152.32.36.xx /27, 152.32.37.xx /27.

2.- Estudio de direcciones IP

- **Investigación de las computadoras**

✓ Lo primero a realizar es una investigación de todas las computadoras de la SUGEF, analizando 3 aspectos: dirección IP, sistema operativo y dirección MAC.

✓ La tarea se debe ir realizando por departamentos y en donde esta tarea solo toma como máximo 5 minutos por usuario. La información se encuentra en:
✓ Inicio
✓ Ejecutar
✓ Escribir winipcfg y dar un click en aceptar.
✓ En el botón more info dar un click
✓ Mandar a imprimir esta información (imprimir pantalla) y no olvidar de colocar el nombre del usuario de esa computadora.

- **Investigación de las impresoras**

La tarea a realizar es la siguiente: Identificar por departamento las impresoras que hay y el código que tiene. Algunas tienen escrito la dirección y IP, si no, hay que realizar la investigación en el servidor.

- **Realización del Plan de Acción**

Este plan contempla las variables que se obtuvieron de la investigación de las computadoras y de las impresoras. El plan debe contemplar que la migración a DHCP debe realizarse por departamentos, y hasta que no se concluya un departamento no se puede seguir en el otro.

El plan se puede empezar desde el piso 8 y así sobre todos los departamentos de cada piso hasta llegar al piso 3. El tiempo ha programar por departamento se debe establecer de acuerdo a varios aspectos:

- ✓ 10 minutos por usuario en donde el sistema operativo sea windows 98 o alguna versión más nueva.
- ✓ Si hay que actualizar el sistema operativo (usuarios con windows 95), la actualización y cambio a DHCP del usuario puede tardar hasta 40 minutos.
- ✓ Como algunos clientes (auditores o supervisores) tienen que salir constantemente del edificio, hay que contemplar que la mayoría de usuarios se encuentren el día en que se vaya a realizar el cambio en el departamento o avisarles para que en su medida, puedan estar ese día y brindarles prioridad.
- ✓ Determinar el número de personas que hay para realizar este cambio, en cada día, debido al rol del Departamento de Soporte Técnico.

3.- Servidor

En el servidor solo se debe agregar los rangos direcciones IP en que el administrador desee que otorgue el DHCP

4.- Migración

- ✓ Una primera etapa a realizar es la migración de ***direcciones estáticas*** de las impresoras hacia el nuevo perfil H.1 y H.2, dedicado a este grupo. Por una utilización más optima, la literatura recomienda que a las impresoras se le asigne un bloque de direcciones estáticas.
- ✓ Realizar el cambio de direcciones estáticas a dinámicas en las computadoras de la SUGEF, de acuerdo al plan realizado, con la política de autenticación con MAC addreess.
- ✓ Realizar la creación de las nuevas VLAN de acuerdo a la propuesta de la red, en las direcciones 152.32.33.xx /27 y 152.32.34.xx /27.
- ✓ Paralelamente se debe ir cambiando las direcciones IP a los servidores y también la dirección DNS y WINS, de acuerdo a la propuesta de red. Se debe tener en cuenta que a los servidores se le debe colocar una ***dirección IP estática.***

5.- Monitoreo

- ✓ Realizar pruebas de carga en la red, para comprobar que los diferentes enlaces están funcionando correctamente, o también, contratar el servicio de un sneefer para analizar el comportamiento de la red, y además tener una base del comportamiento del sistema ante las nuevas aplicaciones que se van a implementar.

6.1.6 Diseño de VoIP

a.- Asignación de direcciones IP

Se tomó la política de diferenciar la información entre datos y voz en lo referente a VLAN, por lo que, se escogió tomar todo un nuevo grupo de direcciones diferentes a las que ya se han asignado a cada usuario de la red.

Para ello, en primera instancia es necesario que la SUGEF agregue dos nuevos grupos de direcciones IP cada una de 256 usuarios, para ser usadas única y exclusivamente para implementar la red de voz sobre direcciones IP.

Las direcciones que se mencionan aquí son solo para efectos de ejemplificación, porque la decisión final la toma el administrador de la red en el momento en que se vaya a implementar la red de telefonía.

Estas direcciones son la 152.32.38.xx /27 y 152.32.39.xx /27, tomando en cuenta el criterio de diseño de realizar el subneteo lo más pequeño y conveniente, para evitar problemas ya mencionados anteriormente.

La tabla 6.9 y tabla 6.10 muestra como están siendo distribuidas las direcciones por subneteo:

Tabla 6.9 Direccionamiento IP de la dirección 152.32.38.xx /27

SUBNET	SUBNET MASK	NETWORK NUMBER	BROADCAST NUMBER
1	255.255.255.224	152.32.38.0	152.32.38.31
2		152.32.38.32	152.32.38.63
3		152.32.38.64	152.32.38.95
4		152.32.38.96	152.32.38.127
5		152.32.38.128	152.32.38.159
6		152.32.38.160	152.32.38.191
7		152.32.38.192	152.32.38.223
8		152.32.38.224	152.32.38.255

Tabla 6.10 Direccionamiento IP de la dirección 152.32.39.xx /27

SUBNET	SUBNET MASK	NETWORK NUMBER	BROADCAST NUMBER
1	255.255.255.224	152.32.39.0	152.32.39.31
2		152.32.39.32	152.32.39.63
3		152.32.39.64	152.32.39.95
4		152.32.39.96	152.32.39.127
5		152.32.39.128	152.32.39.159
6		152.32.39.160	152.32.39.191
7		152.32.39.192	152.32.39.223
8		152.32.39.224	152.32.39.255

Las siguiente tabla (6.11) muestra las direcciones que no van a ser utilizadas porque son asignadas al router de cada piso del edificio además de que la subnet 1 y la subnet 8 de los dos grupos de direcciones se identifican como reservadas, ya que por criterios de diseño no se recomienda utilizar estas subnets.

Tabla 6.11 Distribución de direcciones de Router por piso

VLAN	***2 ****	***3****	***4****
PISO 3	152.32.38.33	152.32.38.65	152.32.38.97
PISO 4	152.32.38.34	152.32.38.66	152.32.38.98
PISO 5	152.32.38.35	152.32.38.67	152.32.38.99
PISO 6	152.32.38.36	152.32.38.68	152.32.38.100
PISO 7	152.32.38.37	152.32.38.69	152.32.38.101
PISO 8	152.32.38.38	152.32.38.70	152.32.38.102

***** para el grupo de direcciones del router de la dirección 152.32.39.xx /27 se cumple exactamente la misma tabla, lo única que cambia es el 38 por un 39.

Tabla 6.12 Distribución de direcciones de Router por piso

VLAN	***5****	***6****	***7****
PISO 3	152.32.38.129	152.32.38.161	152.32.38.193
PISO 4	152.32.38.130	152.32.38.162	152.32.38.194
PISO 5	152.32.38.131	152.32.38.163	152.32.38.195
PISO 6	152.32.38.132	152.32.38.164	152.32.38.196
PISO 7	152.32.38.133	152.32.38.165	152.32.38.197
PISO 8	152.32.38.134	152.32.38.166	152.32.38.198

* para el grupo de direcciones del router de la dirección 152.32.39.xx /27 se cumple exactamente la misma tabla, lo única que cambia es el 38 por un 39.

La figura 6.12, muestra como se asignó los grupos de direcciones de acuerdo a las políticas de distribución que se van a explicar más delante de acuerdo a los perfiles de usuarios.

	Network Number
RESERVADA	152.32.38.224
USUARIOS 3	152.32.38.192
USUARIOS 2	152.32.38.160
USUARIO 1	152.32.38.128
SECRETARIAS	152.32.38.96
ALTOS CARGOS (desde directores hasta superintende)	152.32.38.64
SERVIDOR-CALL MANAGER	152.32.38.32
RESERVADA	152.32.38.0

	Network Number
RESERVADA	152.32.39.224
NO ASIGNADO 2	152.32.39.192
NO ASIGNADO 1	152.32.39.160
USUARIOS 7	152.32.39.128
USUARIOS 6	152.32.39.96
USUARIOS 5	152.32.39.64
USUARIOS 4	152.32.39.32
RESERVADA	152.32.39.0

Figura 6.12 Distribución de las direcciones IP

b.- Diseño de VLAN

El diseño de las VLAN consiste en agregar las nuevas direcciones de VoIP mostradas en la tabla 6.9 y tabla 6.10 sobre el diseño del modelo lógico de la red propuesta.

Para la VLAN del switch principal (figura 6.12), lo único que se tuvo que hacer fue agregar una nueva VLAN llamada call manager sobre el grupo de servidores, ya que en este VLAN es donde va a estar ubicado el nuevo servidor que se ocupa para controlar y direccionar las llamadas entrantes como salientes.

Para las VLAN de cada piso (figuras del 6.13 al 6.18), el mismo diseño de una se aplica a todas las demás, lo único que cambia es la dirección IP del router interno. El diseño lógico de esta se basa sobre las tablas 6.9 y 6.10, donde cada subred es representada como una VLAN y de cada VLAN de cada piso hay que agregarle una dirección del router interno.

El diseño básicamente tienen las mismas políticas que los diseños anteriores que se encuentran en la propuesta de red y cumple también con las mismas especificaciones de distribución y broadcast, entre otras.

Ya con todo el diseño realizado, se pueden definir la cantidad de usuarios por perfil que se ha definido anteriormente, en la siguiente tabla 6.13:

Tabla 6.13 Cantidad de usuarios por perfil

PERFIL	CANTIDAD DE USUARIOS
Altos Cargos	24
Secretarias	24
Usuarios	138

También en este diseño no se toma en cuenta que existe una subnet dedicada exclusivamente a los servidores que tengan relación con la telefonía de VoIP, además existen también dos subnets de 24 usuarios cada uno, que se encuentran sin asignación como respaldo a que alguno de los perfiles de llene y se necesitaran más direcciones IP.

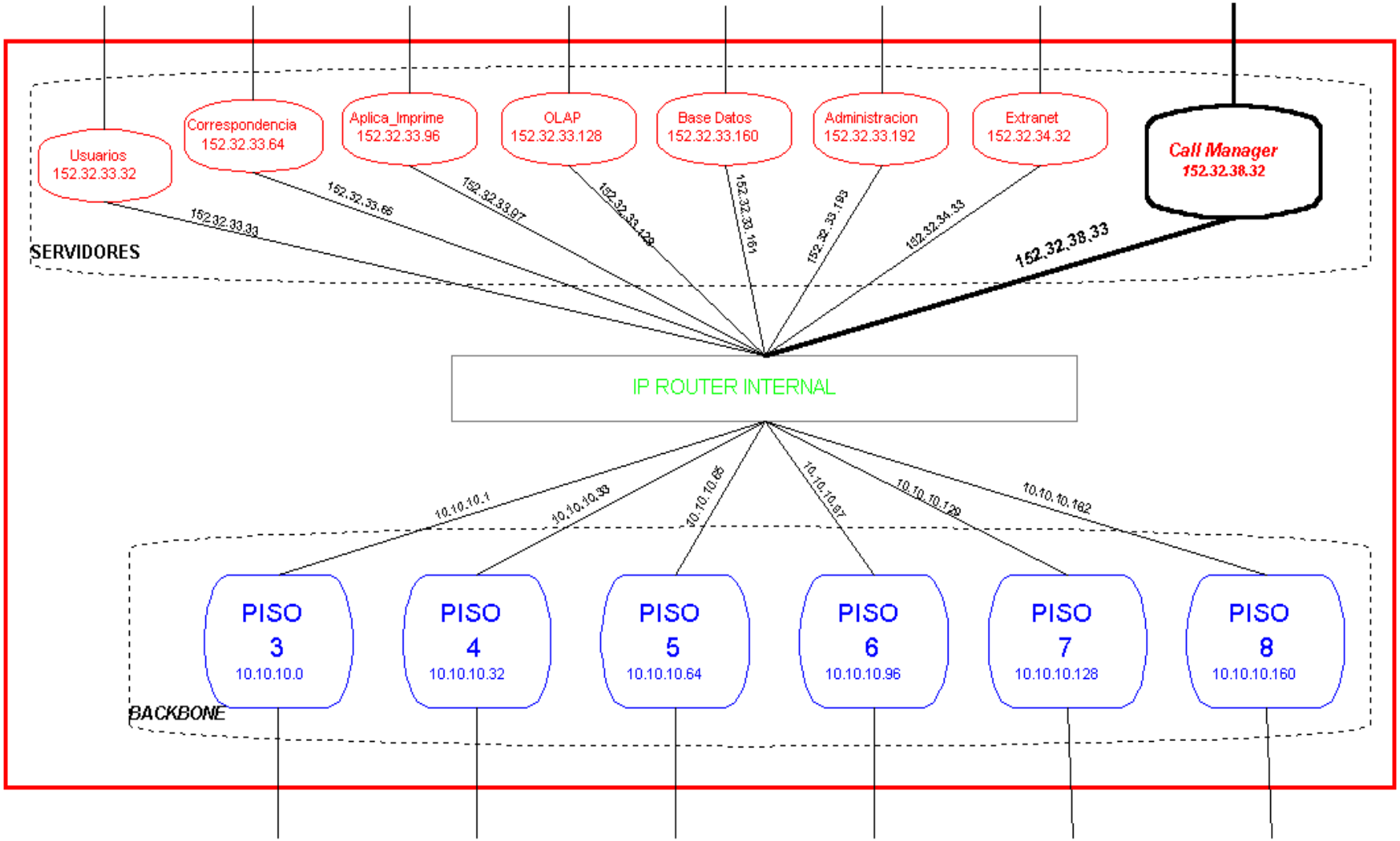


Figura 6.13 Diseño VLAN Switch Principal

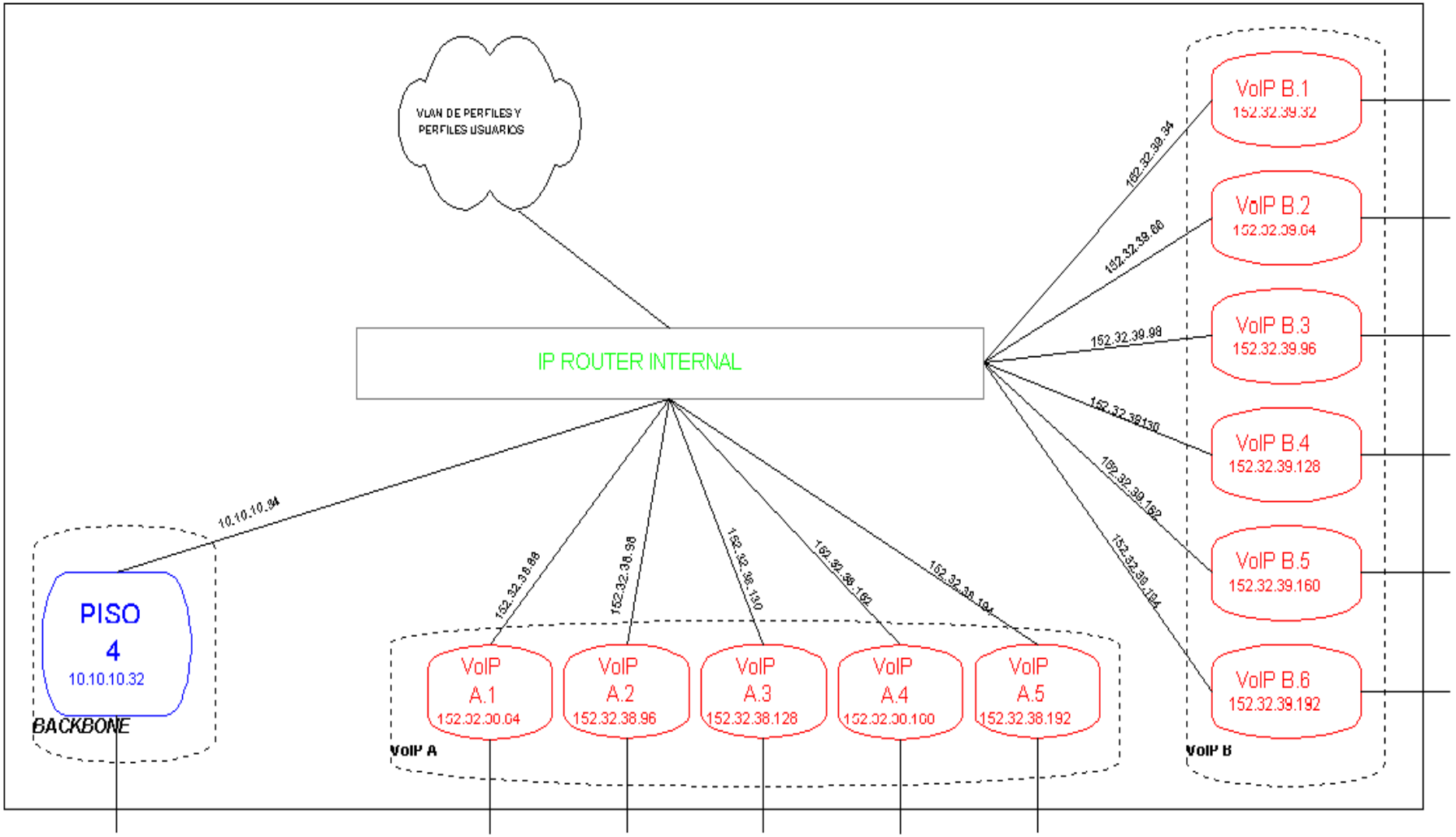


Figura 6.14 Diseño VLAN piso 4 VoIP

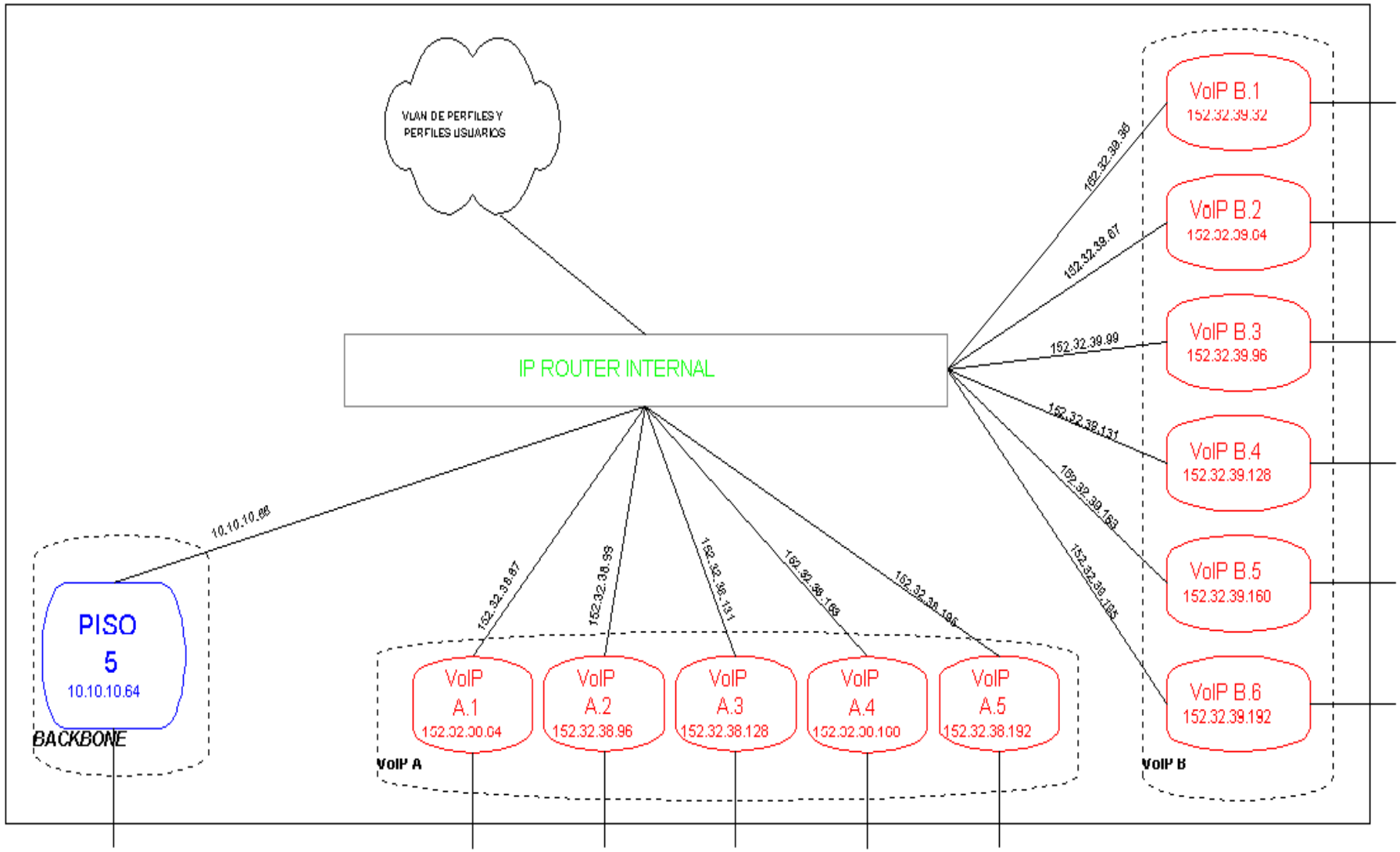


Figura 6.15 Diseño VLAN piso 5 VoIP

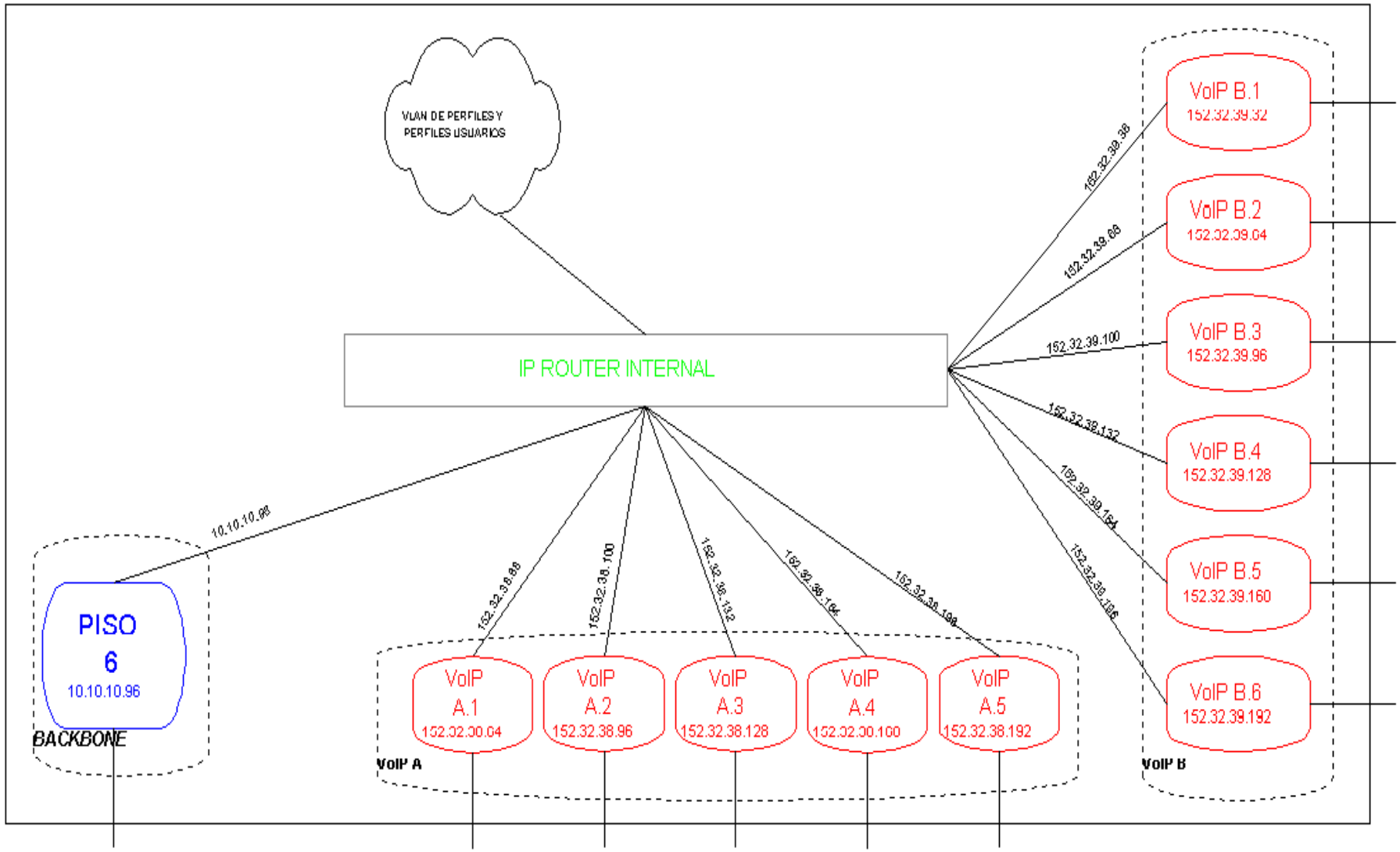


Figura 6.16 Diseño VLAN piso 6 VoIP

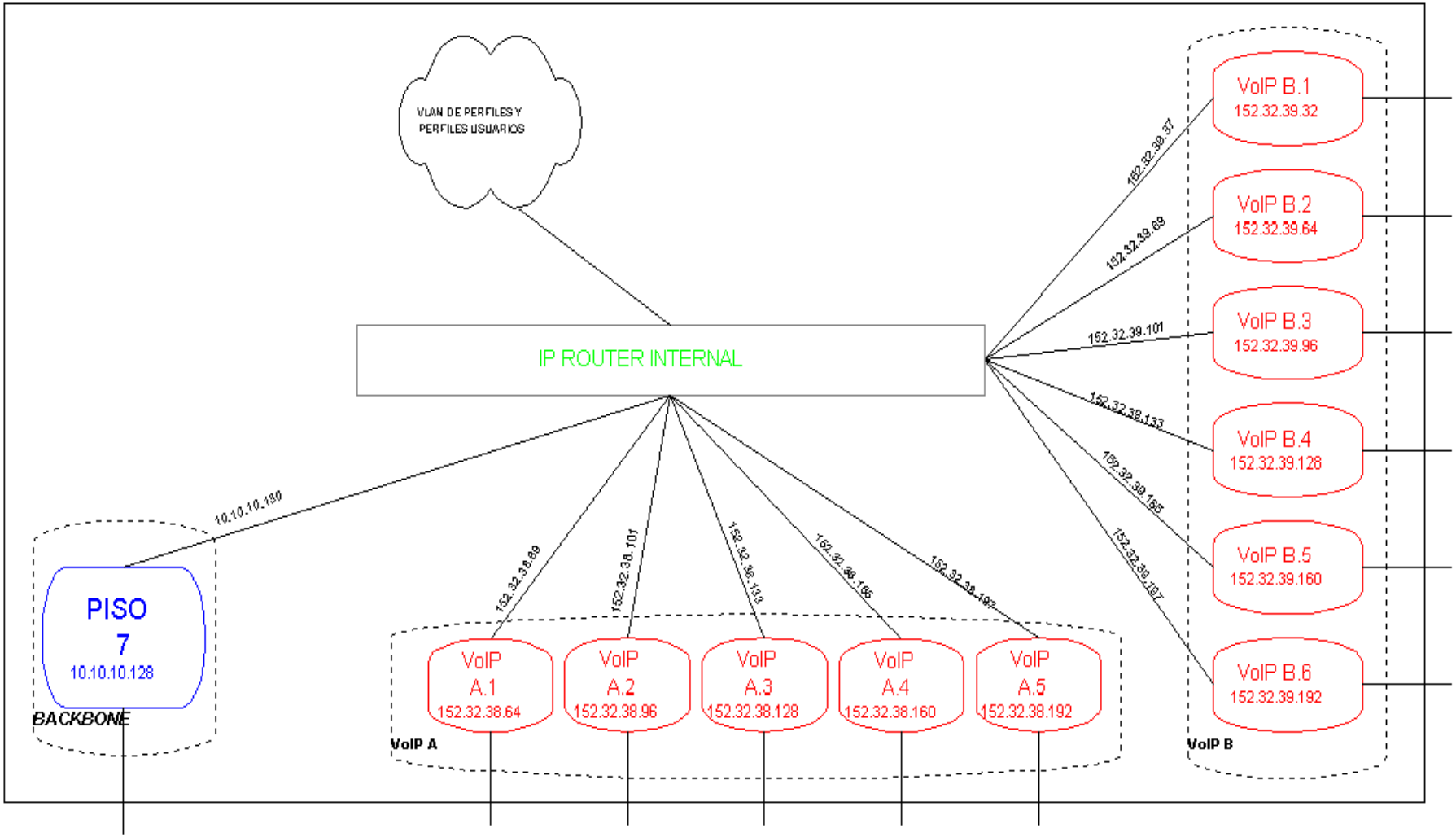


Figura 6.17 Diseño VLAN piso 7 VoIP

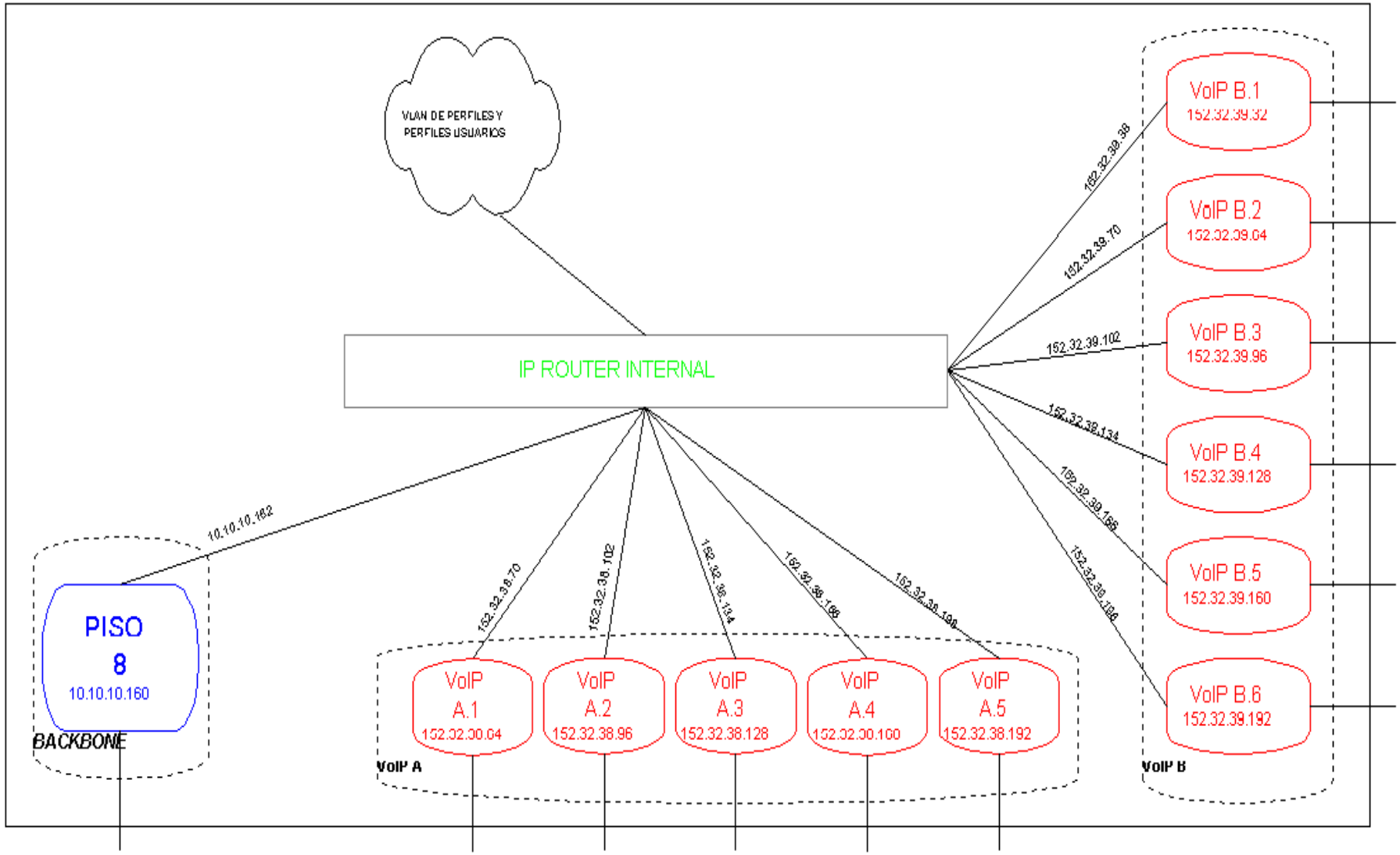


Figura 6.18 Diseño VLAN piso 8 VoIP

c.- Diseño físico de la estructura básica para la red

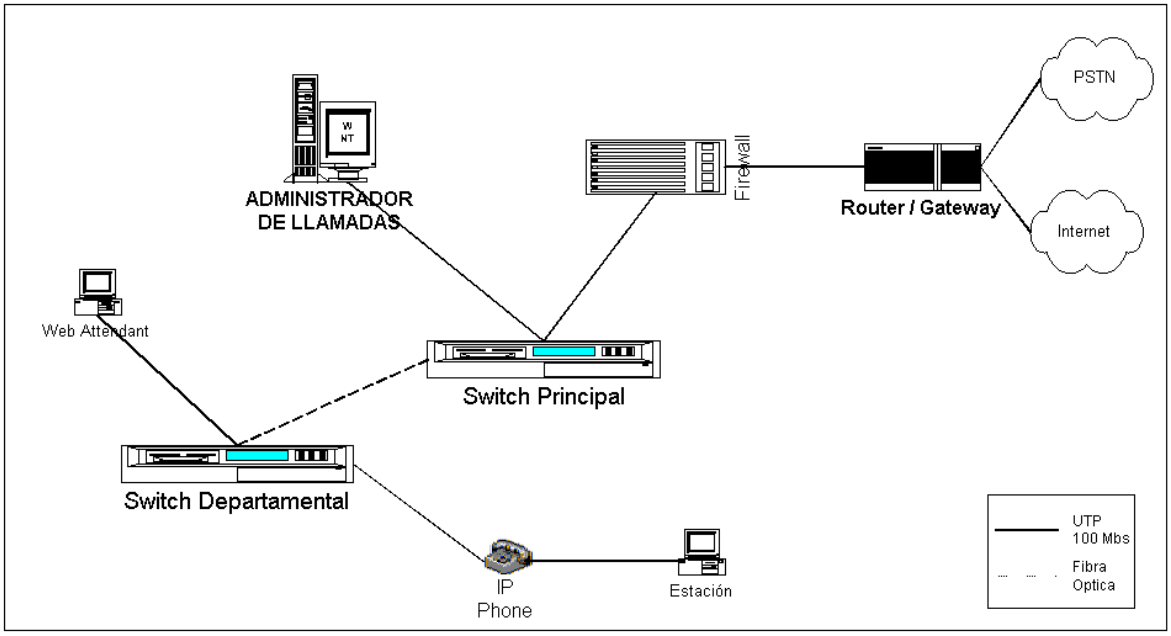


Figura 6.19 Diseño de una red de VoIP

La figura 6.19 presenta la estructura básica de una red de VoIP, donde para lograr un funcionamiento óptimo de la red esta debe contemplar varias características, entre las más importantes están:

- Toda la red debe ser "switchada": significa que se debe asegurar un ancho de banda definido. Se ocupan dispositivos que logren dar esta característica, por lo que cualquier dispositivo como hubs, deben ser eliminados de la red.
- QoS (calidad de servicio): los switches deben ser capaces de identificar los paquetes que se transmiten con voz, y capaces cumplir con las especificaciones básicas de QoS.
- El teléfono de VoIP debe ser capaz de conectarse en serie con la computadora, es decir, que pueda internamente realizar un switch entre voz y datos para no tener que incluir más puertos en los switches, lo que implicaría un mayor costo.
- Debe existir un software de atención a personas que llaman a la central de la SUGEF.

- El servidor de administrador de llamadas debe ser capaz de controlar al menos 500 usuarios de teléfono.
- El router/gateway debe ser capaz de conectarse tanto a Internet como a una red de telefonía pública.

6.2 Alcances y limitaciones

Evaluar los alcances y limitaciones del proyecto es un poco difícil, porque el proyecto ya ha realizado en casi su totalidad de manera teórica. Entonces, se parte del hecho y de la conjetura popular que dice "el papel aguanta todo", con lo que al realizar este proyecto la premisa es que todo se va a cumplir tal y como está escrito, y que no van a existir fallas y si las hay van a ser fallas menores.

La primera parte del proyecto consiste en realizar una migración de todo el direccionamiento IP de la red (máquinas, impresoras y servidores). Además este plan por las características del direccionamiento IP que se escogió, es necesario cambiar el protocolo de enrutamiento. Para llevar a cabo este trabajo es necesario contar con dos factores muy importantes: a) dedicación, que incluye tomar intervalos largos de tiempo para realizar las tareas del redireccionamiento IP y además invertir por lo menos dos fines de semana en cambios con el DHCP y el cambio del protocolo de enrutamiento; b) personal, para llevar a cabo esta tarea es necesario por lo menos contar con tres personas que trabajen en equipo, y que conozcan como realizar las tareas que esta parte requiere.

La segunda parte, consiste en implementar la tecnología de VoIP en la red actual. Por las características antes mencionadas y las recomendaciones que más adelante se hacen, es necesario modificar varias partes de la topología de la red, por lo que es necesario comprar equipo. Como esta entidad es pública, para realizar una compra es necesario cumplir con una serie de requisitos hasta culminar con la licitación, donde todo este proceso dura alrededor de un año y medio.

Entonces, poder realizar una evaluación del proyecto es un poco difícil, por el hecho de que el documentos es teórico y no se ha realizado ninguna parte práctica. Es por ello, que se dificulta evaluar el proyecto y su verdadera evaluación es hasta el momento en que se empieza a implementar prácticamente.

CAPITULO 7
CONCLUSIONES Y RECOMENDACIONES

CONCLUSIONES

- Se determinó que el subneto fue la mejor manera de realizar la división de perfiles y usuarios, sin entrar en el VSLM que sería más eficiente pero más difícil de controlar.
- Al utilizar el subnetting debe cambiarse el protocolo de enrutamiento, ya que el RIP versión 1 no lo soporta.
- Los accesos de cada perfil en las VLAN se realizan por medio de una lista de accesos que permite programar el switch Xylan.
- Se determinó que los accesos por MAC son más seguros, primero para identificar al usuario y luego para el ingreso a su respectiva VLAN.
- Por políticas de diseño y realizarlo más óptimo, se decidió hacer grupos pequeños de perfiles.
- RIP v2 es la opción más óptima para el cambio del protocolo de enrutamiento, por su fácil programación y su diseño a nivel de LAN pequeña.
- Para realizar el cambio de direcciones IP y la migración del protocolo de enrutamiento, es necesario contar con dos factores: dedicación de tiempo y personal.
- La tecnología de VoIP elimina el concepto del uso de una PBX.
- La integración de multiservicios (voz, video y datos) simplifica el trabajo del administrador a un solo sistema y no a varios y diferentes sistemas.

RECOMENDACIONES

- Una recomendación importante sería agregar un nuevo grupo de VLAN la cual se denominaría voz sobre IP porque este es el otro proyecto con que cuenta la SUGEF, este se determinaría a un plazo de 3 años, pero en la segmentación lógica quedaría listo para implementar de una vez.

- Para lograr implementar la tecnología de VoIP, es necesario que todo el equipo de red que se encuentre en la LAN sea capaz de mantener un ancho de banda estable, por lo que los hubs que existen es necesario eliminarlos y comprar un nuevo equipo (switches)

- Entre cada switch departamental y el switch principal existen dos cables de fibra óptica, una manera de aprovechar esta fibra es implementar una línea de fibra para datos y otra línea de fibra para voz.

- Como el equipo de la red actual ya casi cumple su vida útil, es necesario que el equipo que se vaya a comprar soporte tecnologías que se están empezando a integrar, como lo son: soporte gigabit y terabit, protocolo 802.1Q y 802.1p, equipo escalable en el backplane, convergencia para multiservicios, maneje multicapas (capa 3 y capa 4) y realizar redundancias para conexión entre equipos.

- Al implementar la tecnología de VoIP, se podría pensar de una vez en implementar la tecnología de videoconferencia, ya que cumpliría con los QoS de una vez, y se tendría una mayor integración de multiservicios.

BIBLIOGRAFIA

- Tanenbaum, A. **Redes de Computadoras**. Tercera Edición, Prentice Hall. México, 1997.
- Xylan Corporation. **The switching book II.** Second Edition. U.S.A 1998.
- Xylan Corporation. **User Manual Omniswitch 3.0.** Second Edition. U.S.A 1997.
- Xylan Corporation. **User Manual Advanced Routing.** Second Edition. US.A. 1997.
- Espinoza Kenett. **Diagnóstico de la Red Banacio para diseñar un sistema de monitoreo unificado que administre las plataformas que la compones.** Proyecto Graduación Instituto Tecnológico de Costa Rica, 2000.
- Microsoft Corporation. **Internetworking with Microsoft TCP/IP on Microsoft Windows NT.** Third Edition, Cargraphics S.A.. Colombia 1999.
- Cisco Systems. **CCNA study guide.** Ginger Warner U.S.A., 1999.
- Cisco Systems. **Cisco AVVID - Building an Enterprise IP Telephony Network.** Cisco Seminar Series. U.S.A. 2000.
- Microsoft Corporation. **Instalación e Introducción al TCP/IP en Windows NT.** <http://www.microsoft.com/latam/technet/basicos/art99-001/default2.asp> (21 de Marzo)
- Mind Share Systems. **VSLM Tables.**

  <http://www.mindsharesystems.com/network/net_tech(3).asp> (26 de marzo)

APENDICES Y ANEXOS

Apéndice 1. Distribución Física del Edificio de la SUGEF

Apéndice 2. Distribución de los Dispositivos de la red

NOTA: el apéndice 1 y el apéndice 2 han sido quitados debido a que la entidad consideró que contenía material sensible para que otros empresas o personas la conozcan.

Apéndice 3: Routing Internal Protocol (RIP) version 1

RIP para IP es un protocolo de enrutamiento por vector de distancia que facilita el intercambio de información de enrutamiento IP. Al igual que RIP para IPX, RIP para IP tiene su origen en la versión Xerox Network Services (XNS, Servicios de red de Xerox) de RIP y se convirtió en un protocolo de enrutamiento popular debido a su inclusión en Berkeley UNIX (BSD 4.2 y posteriores) como domonio de servidores enrutadores (un demonio es similar a un servicio de Windows NT 4.0 con RRAS). Hay dos versiones de RIP. La versión 1 (v1) de RIP está definida en RFC 1058 y la versión 2 (v2) en RFC 1723.

RIP y redes grandes

Aunque es simple y está ampliamente admitido, RIP para IP padece algunos de los problemas inherentes a su diseño original basado en LAN. La combinación de estos problemas convierte a RIP en una solución adecuada sólo en redes IP de tamaño pequeño a medio.

RIP y números de saltos

RIP utiliza un número de saltos como medida para la ruta que se almacena en la tabla de enrutamiento IP. El número de saltos es el número de enrutadores que se deben atravesar para llegar hasta la red deseada. RIP tiene un máximo de 15 saltos; por tanto, sólo puede haber 15 enrutadores entre dos hosts cualesquiera. Las redes que tienen 16 o más saltos se consideran no accesibles. Es posible personalizar los números de saltos para configurar los vínculos lentos en varios saltos; sin embargo, el número de saltos acumulados entre dos redes cualesquiera no puede ser superior a 15.

El número de saltos de RIP es independiente del campo TTL (Tiempo de vida) del encabezado IP. En un sistema de redes, normalmente un paquete IP llegaría a una red que se encuentre a 16 saltos si tiene un TTL adecuado; sin embargo, para el enrutador RIP la red será inalcanzable y los intentos de reenviar paquetes a los hosts de la red harán que el enrutador RIP emita mensajes de destino ICMP no accesible o red no accesible.

RIP y entradas de la tabla de enrutamiento

RIP permite la existencia de múltiples entradas en la tabla de enrutamiento de una red si hay múltiples rutas de acceso. El proceso de enrutamiento IP elige la ruta con la medida menor (menos saltos) como la mejor ruta. Sin embargo, las implementaciones típicas de enrutadores de RIP para IP, incluido Windows NT 4.0 con RRAS, sólo almacenan una única ruta de medida menor para cualquier red. Si el RIP recibe varias rutas con número de saltos menor, se almacenará en la tabla de enrutamiento la primera ruta con medida menor que se haya recibido.

Si el enrutador RIP almacenara una lista completa de todas las redes y todas las formas posibles de llegar a cada red, la tabla de enrutamiento podría tener cientos, o incluso miles, de entradas en el caso de una red IP grande con múltiples rutas de acceso. Puesto que sólo se pueden enviar 25 rutas en un único paquete RIP, las tablas de enrutamiento grandes tienen que enviarse como múltiples paquetes RIP.

Anuncio de rutas RIP

Los enrutadores RIP anuncian el contenido de sus tablas de enrutamiento cada 30 segundos en todas las redes conectadas mediante una subred IP y difusión de nivel MAC. (Es posible configurar los enrutadores RIP v2 para realizar multicast (multidifusión) de los anuncios RIP.) Las redes IP grandes tienen la sobrecarga de la

difusión RIP de las tablas de enrutamiento grandes. Esto puede ocasionar problemas en el caso de los vínculos WAN en los que partes significativas del ancho de banda de los vínculos WAN se dedican al tráfico RIP. Como resultado, el enrutamiento basado en RIP no se adapta bien a redes grandes o implementaciones WAN.

Convergencia RIP

De forma predeterminada, a cada entrada de la tabla de enrutamiento aprendida mediante RIP se le asigna un valor de tiempo de espera de tres minutos desde la última vez que se recibió en un anuncio RIP procedente de un enrutador RIP vecino. Cuando un enrutador queda inactivo debido a un error de hardware o software, pueden pasar varios minutos hasta que se propague por la red el cambio de topología. Esta situación se denomina problema de convergencia lenta.

Convergencia en redes RIP

RIP para IP, al igual que la mayoría de los protocolos de enrutamiento por vector de distancia, anuncia sus rutas de forma asincrónica y sin confirmación. Esto puede dar lugar a problemas de convergencia. Sin embargo, puede habilitar modificaciones en los algoritmos de anuncio para reducir el tiempo de convergencia en la mayoría de las situaciones.

Funcionamiento de RIP para IP

El funcionamiento normal de un enrutador RIP para IP consta de un proceso de inicialización (durante el cual el enrutador aprende las rutas de la red gracias a los enrutadores del entorno), un continuo proceso de anuncios periódicos y el anuncio adecuado de las rutas inalcanzables cuando el enrutador queda inactivo debido a una acción administrativa.

Inicialización

Tras el inicio, el enrutador RIP para IP anuncia las redes que tiene conectadas localmente en todas sus interfaces. Los enrutadores RIP del entorno procesan el anuncio RIP y agregan la red o las redes nuevas a sus tablas de enrutamiento.

El enrutador RIP que se está inicializando también envía una solicitud RIP general a todas las redes conectadas localmente. La solicitud RIP general es un mensaje RIP especial que solicita todas las rutas. Los enrutadores RIP del entorno reciben la solicitud RIP general y envían una respuesta de unicast al enrutador solicitante. Las respuestas se utilizan para crear la tabla de enrutamiento del enrutador RIP que se está inicializando.

Mantenimiento continuo

De forma predeterminada, cada 30 segundos el enrutador RIP anuncia sus rutas en todas sus interfaces. La naturaleza exacta del anuncio de enrutamiento depende de si el enrutador RIP está configurado para horizonte dividido o para horizonte dividido con rutas inalcanzables. El enrutador RIP también está escuchando en todo momento anuncios RIP de los enrutadores del entorno para agregar o actualizar las rutas de su propia tabla de enrutamiento.

Apagado administrativo del enrutador

Si un enrutador RIP para IP se apaga correctamente mediante una acción administrativa, envía una actualización desencadenada en todas las redes conectadas localmente. La actualización desencadenada anuncia las redes disponibles a través del enrutador que tienen un número de saltos es 16 (inalcanzable). Los enrutadores RIP del entorno propagan este cambio de topología a través de la red IP mediante actualizaciones desencadenadas.

Como enrutadores dinámicos, los enrutadores RIP para IP también reaccionan a los cambios de la topología de red por vínculos o enrutadores inactivos.

Enrutador inactivo

Si un enrutador queda inactivo debido a un corte de energía u otro error de hardware o software, no tiene la posibilidad de informar a los enrutadores del entorno de que las redes disponibles a través de él ya no están disponibles. Para evitar la existencia habitual de redes inalcanzables en las tablas de enrutamiento, cada ruta aprendida por RIP para IP tiene una duración máxima de 3 minutos (de forma predeterminada). Si la entrada no se actualiza por la recepción de otro anuncio en 3 minutos, el número de saltos de la entrada cambiará a 16 y, finalmente, se quitará de la tabla de enrutamiento.

Por tanto, si un enrutador RIP para IP queda inactivo, los enrutadores del entorno tardan hasta 3 minutos en marcar como inalcanzables las rutas aprendidas del enrutador inactivo. Sólo en ese momento propagarán el cambio de topología por toda la red mediante actualizaciones desencadenadas.

Formato de mensajes de RIP v1

Los mensajes RIP están encapsulados en un datagrama UDP (Protocolo de datagramas de usuario) enviado desde la dirección IP de la interfaz del enrutador y el puerto UDP 520 a la dirección IP de difusión de la subred y el puerto UDP 520. El mensaje RIP v1 consta de un encabezado RIP de 4 bytes y de hasta 25 rutas RIP. El tamaño máximo del mensaje RIP es de 504 bytes. Con el encabezado UDP de 8 bytes, el tamaño máximo del mensaje RIP es una carga IP de 512 bytes. La figura A.8 ilustra el formato de los mensajes RIP v1.

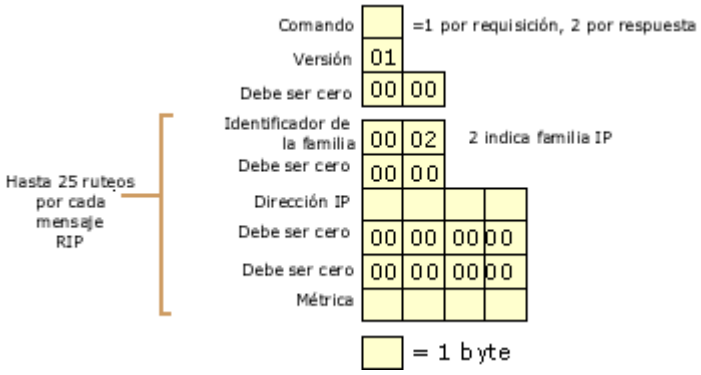


Figura A.7 Formato de los mensajes RIP versión 1

Comando Campo de 1 byte que contiene 0x01 ó 0x02. 0x01 indica una solicitud RIP de todas (una solicitud RIP general) o parte de las tablas de enrutamiento de los enrutadores del entorno. 0x02 indica una respuesta RIP que consta de toda o parte de la tabla de enrutamiento de un enrutador vecino. Se puede enviar una respuesta RIP como contestación a una solicitud RIP, o como un mensaje periódico o de actualización desencadenada.

Versión Campo de 1 byte que se establece con el valor 0x01 para RIP v1.

Identificador de familia Campo de 2 bytes que identifica la familia de protocolos. Se establece con el valor 0x00-02 para indicar la familia de protocolos IP.

Dirección IP Campo de 4 bytes que se establece como el Id. de red IP que puede ser un Id. de red basado en clases, un Id. de red con subredes (anunciado sólo dentro de la red con subredes), una dirección IP (para una ruta de host) o 0.0.0.0 (para la ruta predeterminada). En el caso de una solicitud RIP general, la dirección IP se establece como 0.0.0.0.

Métrica Campo de 4 bytes para el número de saltos a la red IP que debe ser un valor de 1 a 16. La métrica se establece como 16 en una solicitud RIP general o para indicar que la red es inalcanzable en una respuesta RIP (anuncio).

Problemas de RIP v1

RIP v1 se diseñó en 1988 para satisfacer las necesidades de enrutamiento dinámico de las redes IP basadas en tecnología LAN. Las tecnologías LAN de acceso compartido, como Ethernet y Token Ring, admiten difusión de nivel MAC (Control de acceso a medios), donde varios nodos de la red pueden recibir y procesar un único paquete. Sin embargo, en las redes modernas, el uso de difusiones de nivel MAC no es deseable ya que todos los nodos deben procesar todas las difusiones. RIP v1 también se diseñó en un momento en el que Internet aún utilizaba identificadores de red basados en las clases de direcciones Internet. Actualmente, sin embargo, el uso de CIDR (Enrutamiento entre dominios sin clases) y el sistema de subredes de longitud variable es casi necesario para conservar las direcciones IP.

Anuncios RIP difundidos

Todos los anuncios de rutas RIP v1 se dirigen a la subred IP (todos los bits de host tienen el valor 1) y la difusión de nivel MAC. Los hosts que no son RIP también reciben los anuncios RIP. En el caso de redes RIP grandes o muy grandes, la cantidad de tráfico de difusión en cada subred puede llegar a ser importante.

Si bien produce tráfico de difusión adicional, la naturaleza de difusión de RIP v1 también permite el uso de RIP silencioso. Un equipo RIP silencioso procesa los anuncios RIP pero no anuncia sus propias rutas. Es posible habilitar RIP silencioso en los hosts que no son enrutadores para crear una tabla de enrutamiento mucho más detallada que los enrutadores RIP. Al haber rutas más detalladas en la tabla de

enrutamiento, un host RIP silencioso puede tomar mejores decisiones de enrutamiento.

Máscara de subred no anunciada con la ruta

RIP v1 se diseñó para las redes IP basadas en clases, donde el Id. de red puede determinarse a partir de los valores de los 3 primeros bits de la dirección IP de la ruta RIP. Como la máscara de subred no se incluye con la ruta, el enrutador RIP debe determinar el Id. de red basándose en un conjunto limitado de información. Para cada ruta de un mensaje RIP v1, el enrutador RIP v1 lleva a cabo el proceso siguiente:

- Si el Id. de red concuerda con las clases de direcciones (Clase A, Clase B o Clase C), se supone la máscara de subred basada en clases predeterminada. Si el Id. de red no concuerda con la clase de direcciones, entonces:
- Si el Id. de red concuerda con la máscara de subred de la interfaz en la que se recibe, se supone la máscara de subred de la interfaz en la que se recibió.
- Si el Id. de red no concuerda con la máscara de subred de la interfaz en la que se recibió, se supone que el Id. de red es una ruta de host con la máscara de subred 255.255.255.255.

Como resultado de las suposiciones enumeradas anteriormente, las rutas de superredes pueden interpretarse como Id. de red únicos en vez del intervalo de identificadores de red para el que están diseñadas representar y las rutas de subred anunciadas fuera del Id. de la red que se está dividiendo en subredes pueden interpretarse como rutas de host.

Como mecanismo para admitir entornos con subredes, los enrutadores RIP v1 no anuncian las subredes de un Id. de red basada en clases con subredes fuera de la región de subredes de la red IP. Sin embargo, puesto que el Id. de red basada en clases sólo se anuncia fuera del entorno con subredes, las subredes de un Id. de red

en un entorno RIP v1 deben ser contiguas. Si las subredes de un Id. de red IP no son contiguas, lo que se denomina subredes disjuntas, enrutadores RIP v1 independientes anuncian en distintas partes de la red el Id. de red basada en clases. Como resultado de ello, es posible reenviar el tráfico IP a la red incorrecta.

Sin protección frente a enrutadores RIP no autorizados

RIP v1 no proporciona ninguna protección para evitar que un enrutador RIP malintencionado se inicie en una red y anuncie rutas erróneas o imprecisas. Los anuncios RIP v1 se procesan independientemente de cuál sea su origen. Un usuario malintencionado podría utilizar esta falta de protección para sobrecargar los enrutadores RIP con cientos o miles de rutas incorrectas o imprecisas.

Apéndice 4: Routing Internal Protocol (RIP) version 2

RIP versión 2 (v2), como se define en RFC 1723, intenta solucionar algunos de los problemas asociados a RIP v1. La decisión de refinar RIP fue controvertida, dada la aparición de protocolos de enrutamiento más inteligentes y nuevos, como OSPF. No obstante, RIP presenta las siguientes ventajas con respecto a OSPF:

- RIP para IP es fácil de implementar. En su configuración predeterminada más simple, RIP para IP es tan sencillo como configurar direcciones IP y máscaras de subred para cada interfaz de enrutador y, a continuación, encender el enrutador.
- RIP para IP tiene una gran base instalada que consta de redes IP de tamaño pequeño o medio que no desean afrontar la carga del diseño y la configuración de OSPF.

Características de RIP v2

Para que las redes IP actuales minimizaran el tráfico de difusión, utilizaran subredes de longitud variable para ahorrar direcciones IP y aseguraran su entorno de enrutamiento frente a enrutadores mal configurados o malintencionados, se agregaron distintas características clave a RIP v2.

Anuncios RIP con multicast: En vez de difundir anuncios RIP, RIP v2 admite el envío de anuncios RIP a la dirección de multicast IP 224.0.0.9. Los nodos que no son RIP no se ven afectados por el tráfico de anuncios de los enrutadores RIP. Como los anuncios con multicast de RIP v2 se envían a 224.0.0.9 con un TTL de 1, no es necesario el uso de Internet Group Membership Protocol (IGMP, Protocolo de pertenencia a grupos de Internet) para registrar la pertenencia al grupo del host.

La desventaja de esta nueva característica es que los nodos RIP silencioso también deben escuchar el tráfico de multicast enviado a 224.0.0.9. Si utiliza RIP

silencioso, compruebe que los nodos RIP silencioso pueden escuchar anuncios RIP v2 con multicast antes de distribuir RIP v2 con multicast.

El uso de anuncios con multicast es opcional. También se admite la difusión de anuncios RIP v2.

Máscaras de subred Los anuncios RIP v2 envían la máscara de subred junto con el Id. de red. Se puede utilizar RIP v2 en entornos de subredes, de superredes y de máscara de subred de longitud variable. Las subredes de un Id. de red no tienen que ser contiguas (pueden ser subredes disjuntas).

Autenticación RIP v2 admite el uso de mecanismos de autenticación para comprobar el origen de los anuncions RIP entrantes. En RFC 1723 se definió la autenticación por clave de acceso simple, pero existen mecanismos de autenticación más recientes, como Message Digest 5 (MD5, Síntesis del mensaje 5).

Los enrutadores RIP v1 son compatibles con RIP v2 RIP v1 se diseñó teniendo en cuenta su compatibilidad con versiones posteriores. Si un enrutador RIP v1 recibe un mensaje y la versión RIP del encabezado no es 0x01, no descarta el anuncio RIP pero sólo procesa los campos definidos de RIP v1.

Además, los enrutadores RIP v2 envían una respuesta RIP v1 a una solicitud RIP v1, excepto cuando están configurados para enviar únicamente anuncios RIP v2.

Formato de mensajes de RIP v2 Para asegurar que los enrutadores RIP v1 pueden procesar anuncios RIP v2, RIP v2 no modifica la estructura del formato de mensajes RIP. RIP v2 utiliza los campos que en RIP v1 se definieron como Debe ser cero.

El uso de los campos de comando, identificador de familia, dirección IP y métrica son los mismos que los definidos anteriormente para RIP v1. El campo de

versión se establece como 0x02 para indicar un mensaje RIP v2. La figura A.8 ilustra el formato de los mensajes RIP v2.

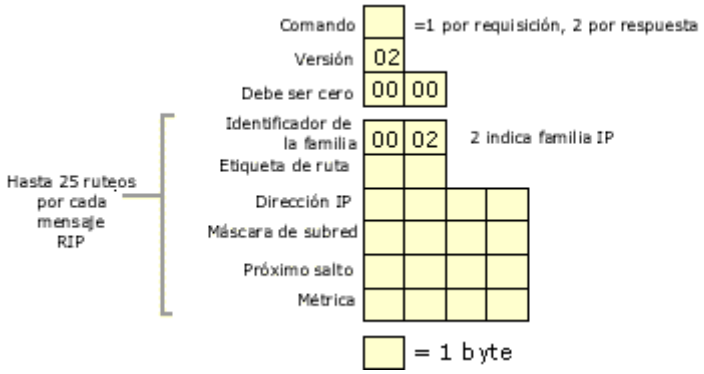


Figura A.8 Formato de los mensajes RIP versión 2

Etiqueta de ruta Este campo se utiliza como método para marcar rutas específicas con propósitos administrativos. Su uso original, tal como se define en RFC 1723, fue distinguir las rutas que estaban basadas en RIP (internas al entorno RIP) de las que no lo estaban (externas al entorno RIP). La etiqueta de ruta es configurable en los enrutadores que admiten múltiples protocolos de enrutamiento.

Máscara de subred Este campo de 4 bytes contiene la máscara de subred del Id. de red en el campo de la dirección IP.

Siguiente salto Este campo de 4 bytes contiene la dirección IP de reenvío (también denominada dirección de puerta de enlace) para el Id. de red en el campo de la dirección IP. Si el siguiente salto se configura como 0.0.0.0, se supone que la dirección IP de reenvío (el siguiente salto) de la ruta será la dirección IP de origen del anuncio de ruta.

El campo de siguiente salto se utiliza para evitar situaciones de enrutamiento que no sean óptimas. Por ejemplo, si un enrutador anuncia una ruta de host para un host que se encuentra en la misma red que la interfaz del enrutador que anuncia la

ruta y no se utiliza el campo de siguiente salto, la dirección IP de reenvío para la ruta de host será la dirección IP de la interfaz del enrutador, no la dirección IP del host. Los demás enrutadores que reciban el anuncio en esa red reenviarán los paquetes destinados a la dirección IP del host a la dirección IP del enrutador que efectúa el anuncio, en vez de reenviarlos al host. Esto crea una situación de enrutamiento que no es óptima.

Al utilizar el campo de siguiente salto, el enrutador anuncia la ruta de host con la dirección IP del host en este campo. Los demás enrutadores que reciban el anuncio en esa red reenviarán los paquetes destinados a la dirección IP del host a la dirección IP del host, en vez de reenviarlos al enrutador que efectúa el anuncio.

Como el campo de siguiente salto se convierte en el campo de dirección de puerta de enlace en la tabla de enrutamiento IP, la dirección IP del campo de siguiente salto debe poderse alcanzar directamente mediante una interfaz de enrutador.

Autenticación en RIP v2 El proceso de autenticación de los anuncios RIP v2 utiliza la primera entrada de ruta del mensaje RIP para almacenar la información de autenticación. Se debe utilizar la primera entrada de ruta, con lo que queda un máximo de 24 rutas en un anuncio autenticado de RIP v2. Para indicar autenticación, el campo de identificador de familia se establece como 0xFF-FF. El campo de tipo de autenticación, normalmente utilizado como el campo de etiqueta de ruta para una ruta, indica el tipo de autenticación que se utiliza. La autenticación por clave de acceso simple utiliza el valor 0x00-11 para el tipo de autenticación.

Los 16 bytes que vienen a continuación del tipo de autenticación se utilizan para almacenar el valor de autenticación. En el caso de la autenticación por clave de acceso simple, el campo de valor de autenticación de 16 bytes almacena la clave de acceso justificada a la izquierda, rellenada con caracteres nulos, con distinción de

mayúsculas y minúsculas y en texto no cifrado. La figura A.9 ilustra el mensaje de autenticación de RIP v2.

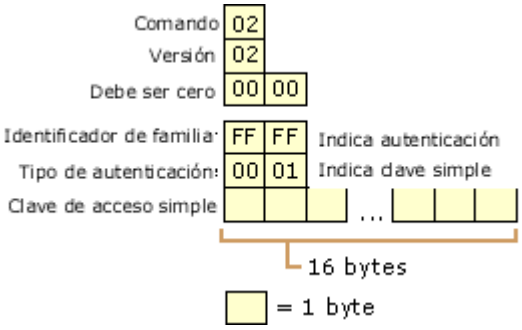


Figura A.9 Formato de mensajes RIP v2 con autenticación

Los enrutadores RIP v1 descartan la primera ruta de un anuncio autenticado de RIP v2 porque el identificador de familia para la ruta es desconocido.

Nota: La autenticación por clave de acceso simple para RIP v2 evita que en la red se coloquen enrutadores RIP no autorizados o mal configurados. Sin embargo, la clave de acceso simple no es segura porque se envía por la red como texto no cifrado. Cualquier usuario con un analizador de protocolos, como Monitor de red de Microsoft, puede capturar los paquetes RIP v2 y ver la clave de acceso de autenticación.

Entornos mixtos de RIP v1 y RIP v2

Se debe tener precaución al utilizar conjuntamente enrutadores RIP v2 y enrutadores RIP v1. Puesto que los enrutadores RIP v1 no interpretan el campo de máscara de subred en la ruta, los enrutadores RIP v2 no deben anunciar rutas que un enrutador RIP v1 pueda interpretar incorrectamente. Las máscaras de subred de longitud variable (VLSM) y las subredes disjuntas no pueden utilizarse en entorno mixtos.

En el caso de una interfaz que utilice RIP v2 para realizar anuncios de modo que los enrutadores RIP v1 puedan procesar las rutas anunciadas, los enrutadores RIP v2 deben resumir las rutas de subred cuando se anuncien fuera de un entorno con subredes. Una ruta de subred específica anunciada a un enrutador RIP v1 puede malinterpretarse como una ruta de host. Además, los enrutadores RIP v2 no pueden anunciar rutas de superredes. Un enrutador RIP v1 malinterpretaría la ruta como una única red, en vez de hacerlo como un intervalo de redes.

Si los enrutadores RIP v2 se encuentran en la misma red que los enrutadores RIP v1, la interfaz del enrutador RIP v2 debe configurarse para difundir sus anuncios. Los enrutadores RIP v1 no procesan los anuncios RIP v2 con multicast.

Solucionar problemas de RIP para IP

Si un entorno RIP está correctamente configurado, los enrutadores RIP aprenden todas las rutas mejores de los enrutadores del entorno después de la convergencia. La lista exacta de rutas que RIP agrega a la tabla de enrutamiento IP depende, entre otros factores, de si las interfaces del enrutador se encuentran o no dentro de una región de subredes, de si se utiliza o no RIP v2 y de si se anuncian rutas de host o rutas predeterminadas.

Pueden producirse problemas con RIP en un entorno mixto de RIP v1 y v2, con el uso de hosts RIP silencioso o cuando todas las rutas RIP adecuadas no se reciben ni se agregan a la tabla de enrutamiento IP.

Rutas incorrectas en un entorno mixto de RIP v1 y RIP v2

En las redes que contengan enrutadores RIP v1, compruebe que RIP v2 está configurado para difundir sus anuncios en redes con enrutadores RIP v1.

En las redes que contengan enrutadores RIP v1, compruebe que las interfaces de los enrutadores RIP v2 están configuradas para aceptar anuncios tanto de RIP v1 como de RIP v2.

Los hosts RIP silencioso no reciben rutas

Si en una red hay hosts RIP silencioso que no reciben rutas del enrutador RIP local, compruebe que los hosts RIP silencioso admiten la versión de RIP. Por ejemplo, si los hosts RIP silencioso sólo admiten escuchar anuncios RIP v1 difundidos, no podrá utilizar la multicast RIP v2.

Los enrutadores RIP no reciben las rutas esperadas

- Compruebe que no distribuye subredes de longitud variable, subredes disjuntas o superredes en un entorno RIP v1 o en un entorno mixto RIP v1 y RIP v2.
- Si está habilitada la autenticación, compruebe que todas las interfaces de la misma red utilizan la misma clave de acceso con distinción de mayúsculas y minúsculas.
- Si se utiliza filtrado de mismo nivel de protocolo RIP, compruebe que están configuradas las direcciones IP correctas para los enrutadores RIP del mismo nivel de protocolo del entorno.
- Si se utiliza el filtrado de rutas RIP, compruebe que los intervalos de Id. de red para el sistema de redes están incluidos o no se excluyen.
- Si los RIP del entorno están configurados, compruebe que están configuradas las direcciones IP correctas para los anuncios RIP por unicast.
- Compruebe que el filtrado de paquetes IP no impide la recepción (mediante filtros de entrada) o el envío (mediante filtros de salida) de los anuncios RIP en las interfaces del enrutador habilitadas para RIP.
- En el caso de las interfaces de acceso telefónico con marcación a demanda que utilicen actualizaciones autoestáticas, configure las interfaces de marcación a demanda para utilizar anuncios de multicast RIP v2. Cuando un enrutador llama a

otro, cada uno recibe una dirección IP del grupo de direcciones IP del otro enrutador, que se encuentran en subredes distintas. Puesto que los anuncios RIP difundidos se dirigen a la dirección de difusión de la subred, cada enrutador no procesa el anuncio difundido del otro enrutador. Con la multicast, los anuncios RIP se procesan independientemente de la subred de las interfaces del enrutador.

Apéndice 5: Open Shortest Path First (OSPF)

Open Shortest Path First (OSPF, Abrir primero la ruta de acceso más corta) es un protocolo de enrutamiento de estado de vínculos definido en RFC 1583. Se diseñó para ejecutarse como un Interior Gateway Protocol (IGP, Protocolo de puerta de enlace interior) para un único sistema autónomo (AS). En un protocolo de enrutamiento de estado de vínculos, cada enrutador mantiene una base de datos con los anuncios del enrutador denominada Anuncios de estado de vínculos (LSA). Las LSA para los enrutadores dentro del sistema autónomo constan de un enrutador, sus redes conectadas y sus costos configurados. Un costo OSPF es una métrica sin unidades que indica la preferencia de utilizar un vínculo. También hay LSA para rutas resumidas y rutas externas del sistema autónomo.

El enrutador distribuye sus LSA a sus enrutadores del entorno. Las LSA se recopilan en una base de datos denominada base de datos de estado de vínculos (LSDB). Al sincronizar las LSDB entre todos los enrutadores del entorno, cada enrutador tiene la LSA del otro en su base de datos. Por tanto, todos los enrutadores tienen la misma LSDB. Desde la LSDB, las entradas para la tabla de enrutamiento del enrutador se calculan mediante el algoritmo de Dijkstra con el fin de determinar la ruta de acceso de menor costo, la ruta de acceso con el menor costo acumulado, a cada red del sistema de redes.

OSPF tiene las siguientes características:

- **Convergencia rápida** OSPF puede detectar y propagar los cambios de topología más rápido que RIP. La cuenta hasta el infinito no se produce con OSPF.

- **Rutas sin loops** Las rutas calculadas por OSPF nunca tienen loops.

- **Escalabilidad** Con OSPF, un sistema autónomo puede subdividirse en grupos contiguos de redes denominados áreas. Es posible resumir las rutas dentro de las áreas para reducir al mínimo las entradas de la tabla de rutas. Las áreas pueden configurarse con una ruta predeterminada que resuma todas las rutas externas al sistema autónomo o al área. Como resultado, OSPF puede adaptarse a redes grandes y muy grandes. Por el contrario, las redes RIP para IP no pueden subdividirse y no se realiza resumen de rutas aparte del resumen de todas las subredes de un Id. de red.

- **Máscara de subred** anunciada con la red OSPF se diseñó para anunciar la máscara de subred con la red. OSPF admite máscaras de subred de longitud variable (VLSM), subredes disjuntas y superredes.

- **Compatibilidad con autenticación** Se pueden autenticar los intercambios de información entre rutas OSPF. Admite autenticación por clave de acceso simple.

- **Compatibilidad con rutas externas** Las rutas externas al sistema autónomo de OSPF se anuncian dentro del sistema autónomo, por lo que los enrutadores OSPF pueden calcular la ruta de menor costo a las redes externas.

Nota La autenticación por clave de acceso simple para OSPF está diseñada para evitar que en la red se coloquen enrutadores OSPF no autorizados. Sin embargo, la clave de acceso simple no es segura porque se envía por la red como texto no cifrado. Cualquier usuario con un analizador de protocolos, como Monitor de red de Microsoft, puede capturar los mensajes OSPF y ver la clave de acceso de autenticación.

Funcionamiento de OSPF

El funcionamiento principal del protocolo OSPF se produce en las siguientes etapas consecutivas y conduce a la convergencia de la red:

a. Compilar la LSDB.
b. Calcular el árbol SPF (Primero la ruta de acceso más corta).
c. Crear las entradas de la tabla de enrutamiento.

Creación de la LSDB mediante anuncios de estado de vínculos

La LSDB es una base de datos con todas las LSA del enrutador OSPF, LSA de resumen y LSA de rutas externas. La LSDB se compila mediante un intercambio continuo de LSA entre los enrutadores del entorno, de forma que cada enrutador está sincronizado con su vecino. Cuando converge el sistema autónomo, todos los enrutadores tienen las entradas adecuadas en su LSDB.

Para crear la LSDB, cada enrutador OSPF debe recibir una LSA válida de cada enrutador del sistema autónomo. Esto se realiza mediante un procedimiento denominado inundación. Cada enrutador envía inicialmente una LSA que contiene su propia configuración. A medida que recibe LSA de otros enrutadores, propaga dichas LSA a sus enrutadores del entorno.

De esta forma, una LSA de un enrutador dado se difunde por el sistema autónomo de modo que los demás enrutadores contienen la LSA de ese enrutador. Aunque parezca que inundar de LSA el sistema autónomo provoca una gran cantidad de tráfico de red, OSPF es muy eficiente a la hora de propagar la información de LSA. La figura A.10 muestra un sistema autónomo OSPF simple, la inundación de LSA entre los enrutadores del entorno y la LSDB.

Los detalles exactos de la sincronización de la LSDB entre los enrutadores del entorno se describe en la sección dedicada a la creación de adyacencias.

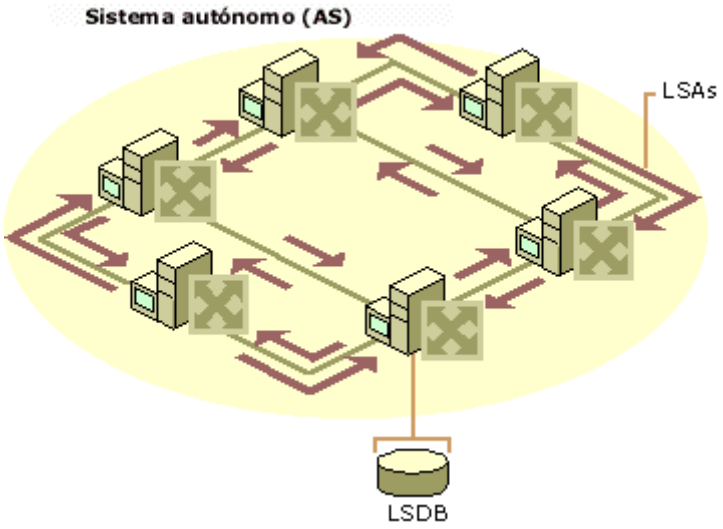


Figura A.10 Base de datos de estado de vínculos (LSDB) OSPF

Id. de enrutador

Para realizar un seguimiento de las LSA que hay en la LSDB, a cada enrutador se le asigna un Id. de enrutador, un número decimal con puntos de 32 bits que es único en el sistema autónomo. El Id. de enrutador identifica el enrutador en el sistema autónomo, no la dirección IP de una de las interfaces del enrutador. El Id. de enrutador no se utiliza como dirección IP de destino para enviar información al enrutador. Es una convención común utilizar como Id. de enrutador la dirección IP mayor o menor asignada al enrutador. Como las direcciones IP son únicas, esta convención asegura que el Id. de enrutador OSPF es único.

Calcular el árbol SPF mediante el algoritmo de Dijkstra

Una vez que se ha compilado la LSDB, cada enrutador OSPF realiza un cálculo de rutas de acceso de menor costo, denominado el algoritmo de Dijkstra, a

partir de la información de la LSDB y crea un árbol de las rutas de acceso más cortas a los demás enrutadores y redes, considerándose a sí mismo como la raíz. Este árbol se denomina árbol SPF y contiene una única ruta de acceso de menor costo a cada enrutador y red del sistema autónomo. Puesto que el cálculo de la ruta de acceso de menor costo lo realiza cada enrutador considerándose a sí mismo como la raíz del árbol, el árbol SPF es distinto para cada enrutador del sistema autónomo.

El algoritmo de Dijkstra procede de una rama de las matemáticas denominada teoría de gráficos y es un método eficaz para calcular un conjunto de rutas de acceso de costo menor relativas a un nodo de origen.

Calcular las entradas de la tabla de enrutamiento a partir del árbol SPF

Las entradas de la tabla de enrutamiento OSPF se crean a partir del árbol SPF y se crea una única entrada para cada red del sistema autónomo. La métrica de la entrada de la tabla de enrutamiento es el costo calculado de OSPF, no un número de saltos.

Para calcular las entradas de la tabla de enrutamiento IP a partir del árbol SPF, se analiza el conjunto SPF{} resultante. El resultado del análisis es una serie de rutas OSPF que contienen el Id. de red IP y su máscara de subred, la dirección IP de reenvío del enrutador vecino adecuado, la interfaz sobre la que es alcanzable el enrutador vecino y el costo calculado por OSPF para la red. Las rutas OSPF se agregan a la tabla de enrutamiento IP.

Apéndice 6: Dynamic Host Control Protocol (DHCP)

Cada equipo de una red TCP/IP necesita tener un nombre y una dirección IP únicos. El Protocolo de configuración dinámica de host (DHCP, *Dynamic Host Control Protocol*) ofrece una forma de simplificar y automatizar este proceso al proporcionar una asignación dinámica de direcciones IP a clientes de la red, independientemente de dónde se encuentren o cuánto se muevan. Esto reduce la carga de trabajo del administrador.

Ventajas del uso de DHCP

DHCP permite la asignación de direcciones IP confiable en una red al reducir la necesidad de asignar manualmente direcciones a cada host. Así, se evitan conflictos de IP que pueden deshabilitar una red.

Los usuarios móviles aprovechan una buena parte de las ventajas de DHCP, que les permite viajar a cualquier parte de la intranet y recibir automáticamente direcciones IP cuando vuelven a conectarse a la red.

Las nuevas características de DHCP proporcionan una forma más flexible y extensible de asignar direcciones IP a equipos host. Las nuevas características se describen en las secciones siguientes.

Informes de servidor: Se puede hacer un seguimiento gráfico de la información acerca del estado general de los servidores DHCP, ámbitos y clientes o "elementos miembro" mediante los iconos que muestra el Administrador de DHCP.

Compatibilidad con ámbito adicional: Una ampliación del protocolo estándar DHCP es compatible con la asignación de direcciones IP de multidifusión que se distribuyen de la misma manera que las direcciones de monodifusión. En DHCP de

multidifusión, los ámbitos de multidifusión se configuran de la misma manera que los ámbitos de DHCP normales, pero en lugar de utilizar direcciones de clase A, B o C, el ámbito de clase D utiliza un intervalo de 224.0.0.0 a 239.255.255.255.

Las aplicaciones características de multidifusión son las conferencias de audio y de vídeo, que normalmente requieren que los usuarios configuren especialmente direcciones de multidifusión. A diferencia de la difusión IP, que necesita ser legible para todos los equipos de la red, una dirección de multidifusión es un grupo de equipos que utiliza la pertenencia al grupo para identificar quién recibe el mensaje.

La característica de asignación de direcciones de multidifusión tiene dos partes: el lado de servidor, que distribuye direcciones de multidifusión; y la interfaz de programación de aplicaciones (API) del lado del cliente, que solicita, renueva y libera direcciones de multidifusión. Para utilizar esta característica, es necesario configurar primero los ámbitos de multidifusión y los intervalos IP de multidifusión correspondientes en el servidor a través del complemento DHCP. A continuación, las direcciones de multidifusión se administran como direcciones IP normales y el cliente puede llamar a las API para solicitar una dirección de multidifusión de un ámbito.

Integración de DHCP y DNS: Los servidores de nombres de dominio proporcionan resolución de nombres para los recursos de red y están estrechamente relacionados con los servicios de DHCP. Los servidores y clientes DHCP se pueden registrar con el protocolo de actualización dinámica DNS. La integración de DHCP y DNS permite el registro de tipo A (nombre a dirección) y puntero (PTR), o registros de dirección a nombre. Esto permite que el servidor DHCP actúe como un proxy en nombre de los clientes Windows 95 y Windows NT 4.0 Workstation con el propósito registrar actualizaciones dinámicas en Active Directory.

Compatibilidad dinámica para clientes del protocolo Bootstrap: Los servidores DHCP responden a solicitudes de protocolo Bootstrap (BOOTP) y a solicitudes de DHCP. BOOTP es un estándar TCP/IP [RFC 951] establecido para la configuración de hosts anterior a DHCP. BOOTP se diseñó originalmente para permitir la configuración de inicio de estaciones de trabajo sin disco. Estas estaciones de trabajo tienen una capacidad limitada para almacenar y recuperar localmente direcciones IP y otra información configurable que es necesaria durante el proceso de inicio para unirse a una red basada en TCP/IP.

Con la nueva compatibilidad con BOOTP dinámico, se puede designar un conjunto de direcciones para clientes BOOTP de la misma manera en que se utiliza un ámbito para clientes DHCP. Así, las direcciones IP se pueden administrar dinámicamente para su distribución a clientes BOOTP. Además, esto permite que el servicio DHCP pueda reclamar las direcciones IP utilizadas en el conjunto de direcciones BOOTP dinámicas, una vez comprobado que transcurrió el tiempo de concesión especificado y que el cliente BOOTP todavía está utilizando cada una de las direcciones.

Acceso de consola de sólo lectura al Administrador de DHCP: Esta característica proporciona un grupo de usuarios local con un propósito especial, el grupo Usuarios de DHCP, que se agrega al instalar el servicio DHCP. Al utilizar la consola del Administrador de DHCP para agregar miembros a este grupo, puede proporcionar acceso de sólo lectura a información relativa a los servicios DHCP en un equipo servidor a usuarios que no sean los administradores. Así, un usuario que pertenece a este grupo local puede ver, aunque no modificar, la información y las propiedades almacenadas en un servidor DHCP específico. Esta característica es útil para los escritorios de Ayuda cuando necesitan extraer informes del estado de DHCP. El acceso de lectura y escritura sólo se puede conceder a través de la pertenencia al grupo Administradores de DHCP.

Apéndice 7: Acrónimos y Abreviaturas

A

AN **Access Node**
AS **Autonomous System**
ATM **Asynchronous Transfer Mode**

B

VER **Bit Error Rate**

C

CCV **Conexión de Canal Virtual**

D

DHCP **Dynamic Host Control Protocol**
DNS **Domain Name Server**

E

EIR **Rango de Información Excedida (*Excess Information Rate*)**

F

FDDI **Interface de Distribución por Fibra(*Fiber Distributed Data Interface*)**

G

GUI **Interface Gráfica de Usuario(*Graphical User Interface*)**

H

HDLC **Control de Enlace de datos de Alto Nivel(*High Level Data Link Control*)**

I

IGMP **Internal Group Membership Protocol**
IGP **Interior Gateway Protocol**
IP **Internet Protocol**

L

LSDB **Link State Data Base**

M

MAC **Control de Acceso a los Medios(*Media Access Control*)**
MIB **Administración de Base de Datos(*Management Information Base*)**

N

NNI **Interface Red-Red(*Network to Network Interface)***
NNM **Nodo de Administración de Redes(*Network Node Manager*)**

O

OSI **Interconexión de Sistemas Abiertos(*Open Systems Interconnection*)**
OSPF **Open Shortest Path First**

R

RIP **Routing Internal Protocol**
RFC **Request For Comments**

S

SNMP **Protocolo de Administración de Redes Simple**
SRS **Especificaciones de Requerimientos de Software**

T

TCP/IP **Protocolo de Control de Transmisión/Protocolo de Internet(*Transmisión Control Protocol y el Internet Protocol*)**
TDM **Multiplexación del Tiempo de División(*Time Division Multiplexing*)**
TTL **Time To Live**

U

UDP **User Datagram Protocol**
UNI **Interface Usuario-Red(*User to Network Interface*)**

V

VLAN **Red Virtual LAN(*Virtual LAN*)**
VPC **Ruta de Conexión Virtual (*Virtual Path Connection*)**
VLSM **Variable Lenght Subnet Mask**

W

WAN **Red de Área Ancha(*Wide Area Network*)**

U

UDP **Protocolo de Usuario (*User Datagram Protocol*)**
UTP **Protocolo Universal de Trunkeo(*Universal Trunking Protocol*)**

Apéndice 8: Glosario

A

Administrador Nodo que participa activamente en la admiinistración de una red, solicita e interpreta datos acerca de dispositivos de red y tráfico, y típicamente interactúa con los usuarios para llevar a cabo sus requerimientos. Los administradores son frecuentemente implementados como aplicaciones de red.

Agente Software que reside en un nodo de red y es responsable de comunicarse con los administradores considerando el nodo. Un agente tiene dos propósitos: responder a las solicitudes de los administradores, suministrando o cambiando los valores de las variables de los objetos según se solicitaron y generar alarmas para alertar a los administradores de los eventos notables que ocurren en el nodo.

Algoritmo Regla o proceso definido para solucionar un problema. En redes es usado para determinar la mejor ruta de tráfico entre dos puntos particulares.

Ancho de Banda Rango de frecuencia disponible en el medio. Es comparable a los carriles de una carretera; entre más ancha sea la carretera, más tráfico podrá circular. El ancho de banda puede ser un solo canal (*basaband*) o puede consistir de muchos canales (*broadband*). Este se mide por el rango de frecuencias (*medidas en Hertz, Ciclos eléctricos por segundo*). Un ancho de banda con muchos canales de frecuencia permitirá que más datos sean transmitidos al mismo tiempo que los que podrían transmitirse con un ancho de banda de una sola frecuencia.

ASCII American Standard Code Information Interchange. Código de bits para la representación de un carácter.

Atenuación Efecto que se presenta cuando las señales se van debilitando al ir viajando a través del cable. A medida que las señales se debilitan, se incrementa la interferencia eléctrica externa y ocurren errores. Para mejorar la calidad de las señales se usan amplificadores en una transmisión analógica (*frecuencias de radio*) y repetidores para una transmisión digital (*bits*).

ATM *Asynchronous Transfer Mode*. Tecnología que explota el comportamiento intermitente de las fuentes de información, los avances tecnológicos y las características más sobresalientes de las redes de conmutación de circuitos y paquetes. Se define como una tecnología para la transferencia de información entre redes de datos.

B

Backbone Parte de una red utilizada como ruta primaria para la transportación del tráfico entre segmentos de redes.

Backplane Conexión física entre la interfase del procesador o tarjeta y el bus de datos y el bus de distribución.

Broadcast Domain Se conoce también como dominio de colisión. Es un grupo de dispositivos que recibirán paquetes originados de cualquier dispositivo que se encuentra dentro de este grupo.

Broadcast Paquete enviado a todos los dispositivos de la red.

D

Dirección de Broadcast Dirección especial reservada para mandar paquetes a todas las estaciones.

Dirección de máscara Combinación de bits usado para describir cual porción de una dirección se refiere a una red o subred.y cual parte al host. Se conoce también como máscara.

Dirección IP asignación de 32 bits a un host utillizando TCP/IP. Puede ser de varias clases (A, B, C, D) y cada dirección contiene número de red, número de red (opcional), y un número de host.

Dominio de Colisión Vease Broadcast domain.

E

Ethernet Especificación de una LAN desarrollada por Xerox, Intel y Digital Equipment Corporation. Las redes Ethernet utilizan CSMA/CD para transmitir paquetes a una velocidad de 10 Mbps sobre una variedad de cables.

Encriptación Aplicación de un algoritmo específico en los datos para alterar la apariencia haciendola incomprensible a aquellos que no están autorizados a ver la información.

F

Frame Relay El Frame Relay es un protocolo estándar para LANs interconectadas, las cuales proveen un método rápido y eficiente de transmisión de datos desde un dispositivo usuario hasta puentes y routers de una LAN.

Fast Ethernet Especificación de velocidad en la red de 100 Mbs.

Fibra Optica Medio físico capaz de transmitir luz modulada. Comparado con otros medios es más caro pero no es susceptible a la interferencia electromagnética y conduce a mayor rangos de transmisión.

Firewall Servidor(es) de accesos o router(es) designados como un buffer entre una red pública y una red privada. Un firewall utiliza listas de acceso y otros métodos para la seguridad de la red privada de dispositivos no autorizadas.

Full Duplex Sistema que permite a los paquetes de información ser transmitidos y recibidos al mismo tiempo, lo que duplica su capacidad a través del enlace.

G

Gateway En la comunidad IP, y en términos anteriores se referían a dispositivos de ruteo**.** Hoy en día, el término router es utilizado para describir nodos que ejecutan esa función, y gateway se refiere a dispositivos de propósito especial que ejecutan conversiones de información en la capa de aplicación de un protocolo a otro.

H

Half Duplex Sistema que permite a los paquetes de información ser transmitidos y recibidos, pero no al mismo tiempo.

Hub Dispositivo que regenera el tráfico de una red LAN, por lo que las distancias de transmisión de una señal pueden ser extendidas. Los hubs son similares a los repetidores, en cuanto a que interconectan LANs del mismo tipo; sin embargo estos interconectan más redes LANs que un repetidor y generalmente son más sofisticados.

Hop Término que describe el paso de paquetes entre dos nodos de la red (por ejemplo: dos routers)

Hop Count Métrica utilizada para determinar la distancia entre la fuente y el destino. RIP utiliza este método.

Host Estación de trabajo en una red. Similar al término nodo excepto que host usualmente implica una estación de trabajo en contrario que nodo se utiliza para definir sistemas de red incluyendo servidores y routers.

I

IGRP Interior Gateway Routin Protocol desarrollado por Cisco para resolver los problemas de direccionamiento en redes grandes heterogeneas.

Interfase Conexión entre dos dispositivos o conexión de red.

IP Protocolo de Internet. IP es un protocolo de capa tres que es estándar para enviar información a través de la red. IP forma parte del conjunto de protocolos TCP/IP que describen el enrutamiento de paquetes de información a los dispositivos direccionados.

M

MAC *Media Access Control*. Protocolo especificado por la IEEE para determinar cuáles dispositivos tienen acceso a la red en algún instante.

MAC address *Media Access Control address*; o también conocida como dirección física. Dirección de capa dos asociada con un dispositivo en particular de la red. Muchos de los dispositivos conectados a una red LAN poseen una MAC address asignada, la cual utilizan para identificar otros dispositivos en la red. La MAC address posee 6 bytes de longitud.

MD5 Message Digest 5. Algoritmo utilizado para la autenticación de mensajes en SNMP v2. MD5 verifica la integridad de la comunicación, autentifica el origen y cheque el tiempo de vida.

Medios de Transmisión Los medios de transmisión sirven para conectar los dispositivos en una red de área local, proporcionando los medios para que las señales de datos viajen de un dispositivo a otro. Algunos medios de transmisión pueden soportar más tráfico que otros. La capacidad de transmisión de datos se mide no sólo por la cantidad de datos que se pueden mandar a través del medio, sino también por qué tan rápido y qué tan lejos pueden viajar los datos sin interferencia o pérdida de fuerza. Los factores que influyen en la transmisión de datos son *ancho de banda*, *interferencia eléctrica* y *atenuación.*

MIB *Management Information Base*. Recopilación de información acerca de las características y parámetros de administración de un dispositivo enlazado. Los MIBs son utilizados por el SNMP para recopilar información acerca de los dispositivos de la red. Los Switches contienen internamente su propia MIB.

Modelo OSI *Open Systems Interconnection*. Es un marco de trabajo para la definición de estándares que enlacen computadoras heterogéneas. Este proporciona la base para la conexión de sistemas "abiertos" (*denota la habilidad de dos sistemas cualesquiera de apegarse al modelo de referencia y a los estándares asociados para conectarse*) para el procesamiento distribuido de aplicaciones.

Modem *Modualtor-demodulator*. Dispositivo que convierte señales digitales y analógicas. En el dispositivo fuente, un modem convierte las señales digitales en una forma conveniente para transmitirla sobre las facilidades que ofrece una comunicación analógica. En el dispositivo destino, las señales analógicas se regresan a su forma digital. Los modems permiten a la información ser transmitida sobre líneas telefónicas.

Multicast Paquetes copiados por la red y enviados a un grupo específico de direcciones

O

OSPF Protocolo sucesor del RIP en internet. Entre sus características están costo de la ruta, multicast y carga balanceada. OSPF fue hecho de una versión del protocolo ISIS.

P

Paquetes Grupo de información que contiene un encabezado que incluye información de control y datos para el usuario. Estos paquetes se encuentran en la capa de red.

PPP *Point to Point Protocol*. Protocolo que está diseñado para enlaces simples los cuales transportan paquetes de información entre dos pares. Este enlace provee una operación simultánea Full Duplex y asume la entrega de los paquetes de información en orden. El protocolo PPP provee una solución simple para una conexión sencilla de una gran variedad de hosts, puentes y routers.

Protocolos de red Los protocolos de red son estándares que permiten la comunicación entre computadoras. Un protocolo típico define cómo las computadoras se deben identificar entre sí en una red, la forma en que los datos deben viajar a través de la red y cómo deberá ser procesada esta información una vez que llegue a su destino final. Los protocolos también definen procedimientos para el manejo de transmisiones perdidas o dañadas. Algunos ejemplos de protocolos de red son IPX, TCP/IP, DECnet, AppleTalk y LAT.

Puentes *Bridges*. Dispositivo que sirve para conectar dos segmentos de la red (WAN ó LAN) en la capa de enlace de datos. Por ser un dispositivo de capa de enlace, los puentes tienen acceso a la información de la dirección física de la estación final.

Dispositivo que interconecta dos redes LANs de diferente tipo para formar una red lógica simple que abarcan dos segmentos de red. Los puentes aprenden cuál terminal (e*ndstation*) se encuentra en cada segmento de red examinando las direcciones fuentes de cada paquete.

Q

QoS Quality of Service (calidad de servicio). Medida del desempeño de una transmisión que se refleja en la disponibilidad de la transmisión.

R

Rebundancia Duplicación de dispositivos, servicios o conexiones que en una causa de fallo de un dispositivo entra a funcinar el segundo dispositivo sin que el usuario se de cuenta del cambio.

Redes LAN *Local Area Network*. Es una red que cubre un área geográfica relativamente pequeña (usualmente no mayor que un grupo local de edificios o un campus de una Universidad, algo así como un radio de 10 km). Las redes LAN necesariamente tienen un diseño sencillo, pueden ser capaces de enlazar cientos de sistemas y dar servicio a varios miles de usuarios. El desarrollo de varios estándares de protocolos de red y medios ha hecho posible la proliferación de LANs en todo el mundo para aplicaciones educacionales y de negocios.

Las redes LANs se caracterizan por altas velocidades de transmisión sobre pequeñas distancias (arriba de 1 km)

Redes WAN *Wide Area Network*. Comunicación de redes que cubre una área amplia. Una WAN puede cubrir una extensa área geográfica, y podría contener algunas redes LANs dentro de ella.

RFC Request for Comments. Serie de documentos utilizados para la comunicación a través de internet. Estos documentos son generados IAB.

RIP Routing Internal Protocol. El más común IGP en el internet. RIP usa el hop count como métrica de ruteo.

RMON Es la abreviación de *Remote Monitoring*, un sistema definido por la IETF que permite monitorear el tráfico de una LAN o una VLAN remotamente.

Es una MIB que permite monitorear remotamente redes LANs direccionando sobre nueve diferentes grupos de información.

Router Dispositivo que provee enlaces WAN entre redes separadas geográficamente.

Dispositivos que tienen acceso a la información desde las tres capas inferiores OSI (*Física, Enlace de Datos y Red*). Se encargan de enviar información a través de la parte interna de la red utilizando información de direcciones lógicas en lugar de físicas. Los routers usan también uno (o más) algoritmos de enrutamiento específicos para calcular el mejor camino a través de la parte interna de la red.

Ruta Estática Ruta que es explicitamente configurada y puesta en la tabla de enrutamiento. Las rutas estáticas tienen preferencia sobre otras rutas que puedan estar en protocolos dinámicos de enrutamiento.

S

Segmentos Sección de una red LAN que está conectado al resto de la red utilizando un puente o un switch.

Servidor Computador en una red que está compartido por múltiples estaciones. Los servidores proveen a las estaciones con acceso a los servicios compartidos tales como archivos de computadora y colas de impresión.

SNMP *Simple Network Management Protocol*. Protocolo estándar de la IETF para administrar dispositivos dentro de una red TCP/IP. Es un conjunto de especificaciones de comunicación de red muy simple que cubre los mínimos necesarios de administración de red exigiendo muy poco esfuerzo a la red sobre la que SNMP está implementada.

Subred Una red compartiendo direcciones particulares de subredes. Subredes son arbitrariamente segmentadas por el administrador de la red para proveer niveles y jerarquías en la estructura de las rutas.

Switch Dispositivo que interconecta varias redes LANs para formar una red LAN lógica simple que abarca algunos segmentos de la red LAN. Los switches son similares a los puentes, en cuanto a que conectan redes LANs de diferente tipo; sin embargo ellos conectan más redes LANs que un puente y generalmente son más sofisticados.

T

Tablas de Enrutamiento Tabla que guarda un router o switcher de capa 3 o algún otro dispositivo que mantiene las rutas de destino de una red en particular y en algunos casos también las métricas.

TCP/IP *Transmission Control Protocol/Internet Protocol*. Este es el nombre de dos de los protocolos más reconocidos para la interconexión de redes. Originalmente un estándar de la UNIX, TCP/IP es ahora soportada sobre casi todas las plataformas, y es el protocolo que emplea la Internet.

TCP contiene la información que viaja a través de la red, asegurándose que la información enviada llegue correctamente a su destino. IP contiene la dirección de la terminal a la cual la información será enviada, así como la dirección de la red destino.

Topología Las redes se pueden organizar en una gran variedad de formas. El cableado de red se caracteriza generalmente como un bus lineal, estrella o anillo; sin embargo, las redes reales, a medida que van creciendo tienden a volverse una combinación de estas topologías. Las redes podrían clasificarse también como centralizadas (*con una computadora central que recibe y transmite todo el tráfico*) o distribuidas (*donde todas las computadoras de la red reciben y transmiten datos*).

Topología de red Se refiere a su cableado físico o disposición. Los tres tipos básicos son: bus, estrella y anillo.

V

VLAN *Virtual LAN*. Grupo de dispositivos que se comunican independientemente de su localización y topología, como si estuvieran dentro de una misma LAN física.

VLSM variable length subnet mask. Habilidad para especificar submáscaras de red de una misma red en diferentes subredes. VSLM puede ayudar a optimizar el espacio disponible.

W

Workgroup Grupo de estaciones de trabajo y servidores en una LAN diseñado para comunicarse e intercambiar datos con otros dispositivos.

Anexos 1: Plataforma X-Vision

X-Vision es un set de estándares basados en herramientas de administración de redes de Switches Xylan para administrar el entorno (*Enterprise*).

Dentro de esta plataforma, al igual que en las otras(Optivity y Magellan), el ambiente gráfico es una herramienta muy útil no solo para aquellas personas encargadas de monitorear la red con ayuda de ésta, sino también para aquellas personas que necesiten obtener el rendimiento estadístico de algún dispositivo específico, por ejemplo.

El contar con una herramienta de monitoreo como la mencionada, permite un manejo más ágil de la información, así como su fácil interpretación y entendimiento.

La ventana principal, la primera en desplegarse corresponde a la figura A.11:

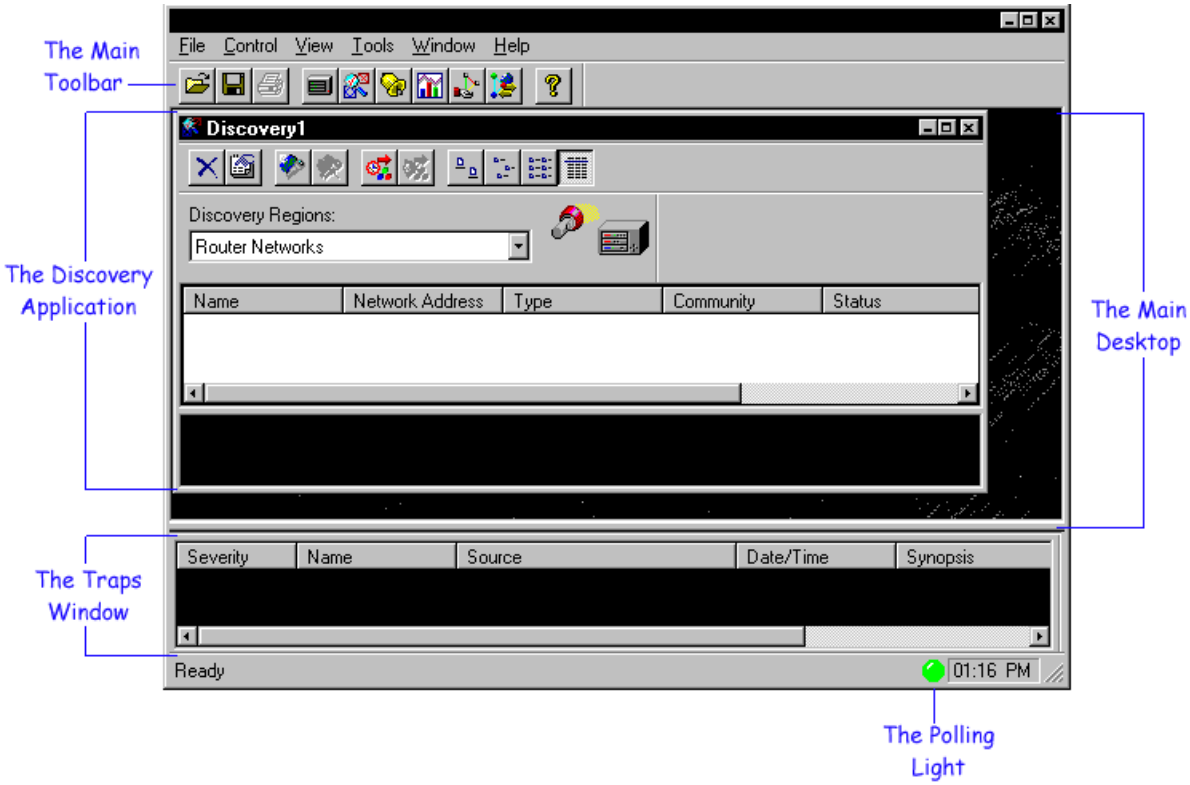


Figura A.11 Ventana principal del X-Vision

Estación de administración integrada de red Xylan

Xylan ofrece dos versiones de X-Vision para ajustarse a sus necesidades:

a. X-Vision para Empresas – para redes extensas

Es una estación NMS integrada y poderosa que tiene como fin administrar switches Omni Switch/Router, X-Cell, PizzaSwitch y OmniStack de Xylan. X-Vision para Empresas está diseñado para configurar los switches, establecer políticas VLAN, realizar estadísticas de la red, crear servicios ATM/WAN y crear conexiones para todos los switches Xylan.

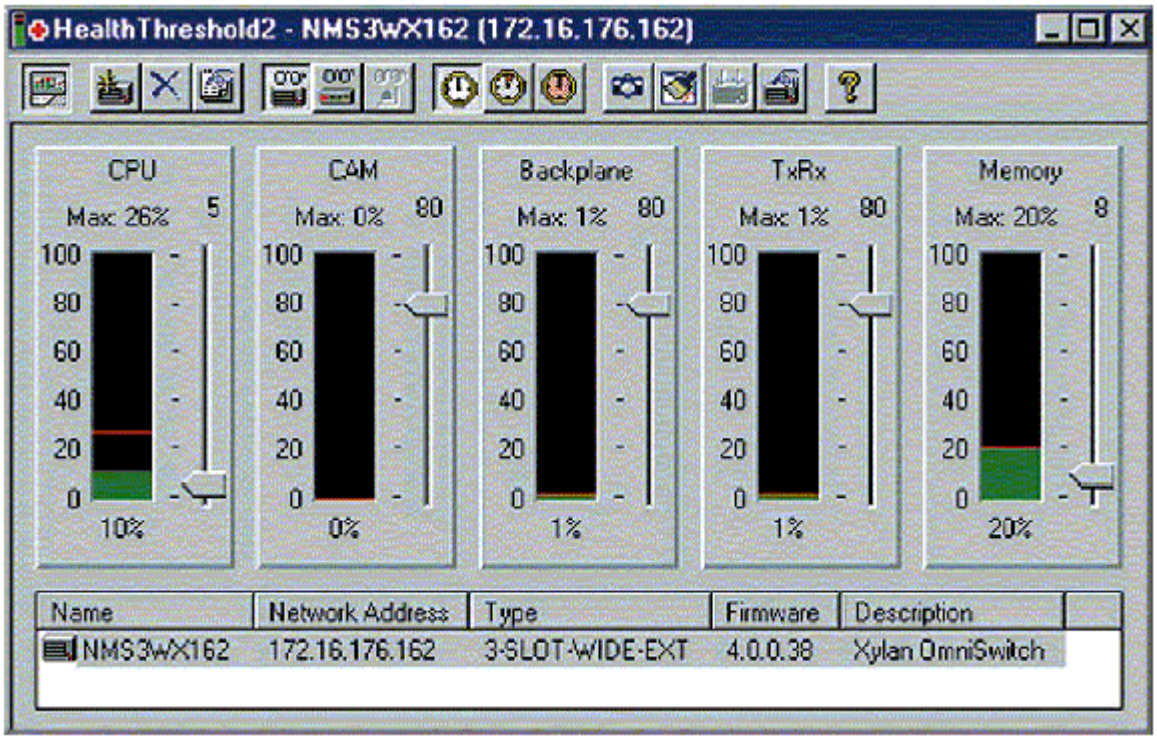


Figura A.12 Pantalla de monitoreo del sistema

A partir de la Figura A.12, se aprecia una de las tantas ventanas que ofrece esta plataforma de monitoreo. En esta se observa el rendimiento de varios dispositivos, como los es el CPU y la memoria, por ejemplo.

Con ayuda de esta ventana, también se pueden establecer parámetros específicos a partir de los cuales se pueden activar alarmas u otro tipo de actividades si no se cumpliesen.

b. X-Vision para Trabajos en Grupo: para redes pequeñas.

X-Vision para Trabajo en Grupo es la opción NMS menos costosa para administración de redes que poseen únicamente los switches PizzaSwitch y Omnistack. Ésta, está diseñada para llevar a cabo la configuración de switches, para el establecimiento de políticas VLAN y para realizar estadísticas de la red, para los switches PizzaSwitch y Omnistack de Xylan.

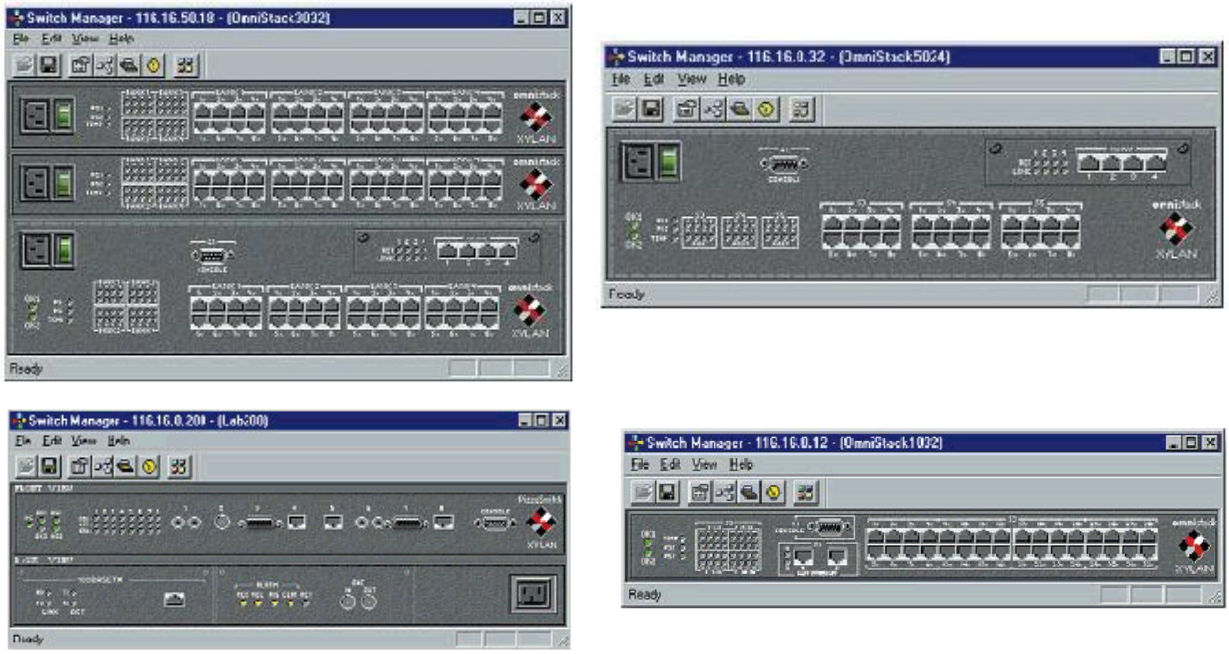


Figura A.13 Representación gráfica del chasis de un switch Xylan OmniStack

A partir de la Figura A.13 anterior, se puede apreciar la representación gráfica del chasis de un switch OmniStack, en la cual están representados cada uno de sus componentes, tal como los puertos.

Al darle “doble clic”, sobre cualquiera de estos componentes se expandirá su correspondiente ventana de monitoreo, en la que se podrán observar sus características y condición actual.

Por otro lado, la versión de X-Vision para UNIX provee las mismas cualidades poderosas que el X-Vision para Empresas pero para los ambientes UNIX (HPUX, Solaris y AIX).

Características y Beneficios

a. Completa conectividad:

   En la banda de comunicación SNMP puede establecerse sobre cualquier enlace de red, incluyendo Ethernet, Fast Ethernet, Gigabit Ethernet, Token Ring, FDDI, ATM o Frame Relay.

b. Auto detección de los dispositivos de la red:

   Detección de los switches Xylan para ser monitoreados.

c. Administración proactiva de la red:

   Permite a los administradores examinar toda la red mientras se toman decisiones de administración de la misma. La información recopilada se puede analizar para asegurarse de que ésta cumpla con los requerimientos del usuario. Los Eventos y los SNMP traps pueden cambiar y recopilarse desde cada switch Xylan, identificando automáticamente los eventos críticos.

d. Control flexible del SNMP para cada dispositivo:

   Los parámetros y configuraciones de los switches se pueden modificar y controlar tanto local como remotamente. Estos parámetros incluyen instalación básica de puertos, servicios ATM, circuitos virtuales Frame Relay, puentes transparentes, fuentes de ruteo, ruteos IP e IPX, servicios de trunking, SNMP traps y configuración RMON.

e. Plataforma de administración simple:

   X-Vision para Empresas administra todos los switches Xylan, permitiendo a los a los administradores utilizar una estación simple para toda la red Xylan, mientras que el X-Vision para Trabajo en Grupo administra todos los OmniStack y los PizzaSwitches.

f. Políticas basadas en administración VLAN:

   Los administradores pueden crear políticas para creaciones dinámicas de VLANs. Las políticas se pueden enviar a un solo switch, a varios o a todos

los switches. Los tipos de VLANs incluyen puertos, MAC address, direcciones de red, protocolos, autenticaciones de usuario o combinaciones entre ellos.

g. Estatus dinámico:

   El tráfico de la red se puede graficar para mostrar los niveles de tráfico dentro de un puerto, dentro del chasis o dentro de un puerto virtual en intervalos definidos por los usuarios. Los administradores pueden observar datos estadísticos, ya sea, de los niveles de tráfico, de las tasas de cambios o variaciones por segundo, esto con niveles de monitoreo mínimos, promedios y máximos que se mantienen durante un período de tiempo. Cabe destacar que la información de múltiples switches se puede desplegar simultáneamente dentro de un solo gráfico.

h. Notificaciones si los niveles de los eventos se exceden:

   Utilizando el correo electrónico (*e-mail*) o algún medio para notificación a través de la red, el software de administración le puede notificar al administrador si algún error crítico se ha presentado. Cualquier archivo ejecutable, como el *paging script*, puede ponerse en ejecución si ocurre un error crítico definido por el usuario.

i. Jerarquía multi-nivel:

   Un análisis categórico de la red, incluyendo ATM PVC, soft PVC y conexiones SVC, se enlistan rápida y lógicamente dentro de una interface de red por tipo, por vista física de switches del módulo y niveles de puerto, configuraciones de servicios, grupos VLAN, nubes WAN y rings.

j. Configuración Drag and Drop:

   Los usuarios pueden “rastrear y bajar” (*drag and drop*) puertos, servicios y conexiones entre elementos del árbol de jerarquías, ya sea en el mapa o sobre el mapa y el árbol.

k. Administración ATM PVC:

   Los administradores pueden utilizar el asistente dirigido para configurar las conexiones PVC a través de su red. Además pueden personalizar cada conexión definiendo variables, tal como la Quality of Service (QoS), propiedades virtuales del canal, AAL-type, prioridad y más.

Administración de los switches

Los administradores de red pueden utilizar X-Vision para configurar, controlar, monitorear y administrar los switches Xylan en sus localidades o remotamente, esto a través de una interface gráfica sencilla (*Graphical User Interface, GUI*). Esto se puede observar a partir de la Figura A.7, la cual, tal y como se explicó representa un esquema del chasis de un switch OmniStack, en el que se muestran cada uno de los componentes del mismo.

La manera en como se lleva a cabo esta administración con ayuda de la GUI es muy simple, pues basta con dar “doble clic” sobre el dispositivo que se desea controlar para lograrlo. Una vez ejecutada dicha acción, se le presentará al administrador una ventana en la que se le mostrarán todas las características del mismo, características que manipulará convenientemente según lo requiera.

X-Vision utiliza el estándar SNMP para configurar los switches sin afectar a los usuarios, ya que la red permanece disponible en todo instante durante las modificaciones que se le hagan a la misma.

Desde una única consola, X-Vision permite a los usuarios configurar fácilmente los puertos físicos Ethernet, Fast Ethernet, Gigabit Ethernet, Token Ring, FDDI, CDDI, Frame Relay y ATM.

Distribución de las políticas basadas en VLANs.

El software y arquitectura de administración VLAN de Xylan, permite a los usuarios crear en pocos minutos VLANs flexibles, escalables y seguras. Los administradores pueden crear VLANs que pueden estar basadas en puertos físicos, MAC address, direcciones layer-three, tipos de protocolos, direcciones multicast, autenticaciones de usuario, *custom bit mask* y/o una combinación de estos tipos de VLAN.

Estas poderosas VLANs no solo reducen los costos de administración asociados con los movimientos de la red, los agregados y los cambios realizados, sino que además permite una mayor flexibilidad y conectividad entre switches de los usuarios. Los usuarios están colocados en VLANs basadas en políticas

definidas por un administrador y los miembros están retenidos detrás de la ubicación física.

Servicios WAN y ATM

X-Vision provee una interface intuitiva que permite a los administradores configurar y controlar sus servicios, mientras proveen una vista de la red. Los administradores pueden administrar cada conexión de red y observar una imagen instantánea de los servicios y conexiones que normalmente están disponibles y en uso.

Debido a que ATM es una conexión orientada a la tecnología, una sencilla configuración vía una poderosa aplicación es extremadamente importante. X-Vision provee una interfase gráfica para servicios de red, y los tipos de conexión incluyen LAN, ATM y WAN. Esta interface sencilla permite a los usuarios administrar y mantener conexiones y servicios de cualquier medio a través de una simple y completa interface.

Monitoreo de la Red

X-Vision utiliza el SNMP para recibir, recoger y almacenar la información de los switches Xylan de toda el ambiente para realizar un diagnóstico proactivo de la red. Esto es poderosamente suficiente para realizar un monitoreo estadístico desde cualquier puerto de los switches Xylan, incluyendo Ethernet, Gigabit Ethernet, Token Ring, FDDI, CDDI y Fast Ethernet, así como ATM y Frame Relay.

X-Vision puede recibir la información de los switches Xylan a través de la LAN y también de la WAN (a través de Frame Relay y ATM). La información recopilada puede ser desplegada por los puertos físicos y switches, o por puertos virtuales, en forma de gráficos de líneas, barras o pastel (*pie*), esto tal y como se aprecia en la Figura A.14.

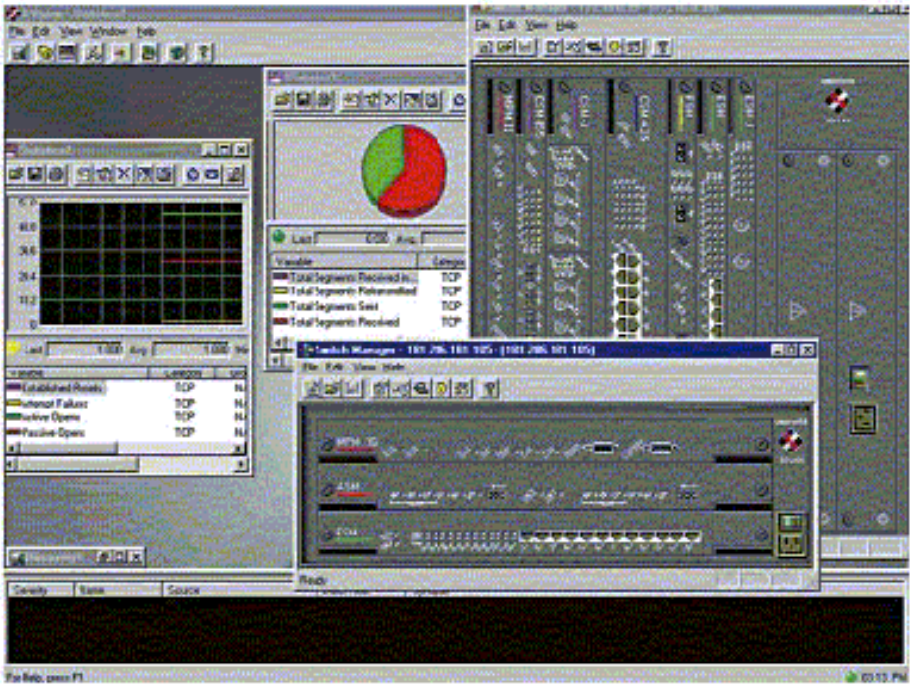


Figura A.14 Monitoreo de puertos de los switches

Requerimientos del Sistema

Los requerimientos del sistema recomendados para operar el X-Vision son:

a. Pentium II a 233 MHz
b. 128 Mb RAM
c. Tarjeta de Video con capacidad para alta resolución (High Color)
d. Monitor de 17", con una resolución a 1024x768
e. 300 Mb de espacio libre en disco
f. Sistema Operativo:

- Microsoft Windows NT 4.0 con Service Pack 3 ó
- Microsoft Windows 98 ó
- Microsoft Windows 95 OSR2.1 (i.e.950B) con DCOM y WinSock2 (DCOM y WinSock incluidos como parte del ejecutable de instalación)

g. Unidad de CD-ROM
h. Tarjeta de Interface de Red
i. TCP/IP Stack